Digital Signature Blindness

Aalberts, B.P.; van der Hof, S.

Publication date:
2000

Digital Signature Blindness

Analysis of legislative approaches toward electronic authentication

Babette Aalberts
Simone van der Hof

Please, quote as: B.P. Aalberts & S. van der Hof, Digital Signature Blindness, *Analysis of legislative approaches toward electronic authentication*, November 1999, <http://cwis.kub.nl/~frw/people/hof/ds-fr.htm>.

Foreword

Back at the beginning of our report yet at the end of an instructive research project, we would like to say thanks to the people that have contributed to this study and the ideas that we have unfolded in it.

We are grateful to Sylvia Huydecoper (CMS Derks Star Busmann Hanotiau), Bert-Jaap Koops (Tilburg University) and Corien Prins (Tilburg University), who have passed valuable comments on earlier drafts of this research report. Their remarks have urged us to further reflection on the subject matter and have contributed to a large extent to the maturing of our notions. Moreover we say thanks to Pascal Kolkman (SENTER), who offered his expertise in the early stage of this research. Also we would like to thank our colleagues at the Center for Law, Public Administration and Informatization who were there to listen to us, discus our ideas and provide the necessary distraction.

In the course of the project we have conducted several interviews in order to gather information and assay our earlier ideas. We would like to say thanks to Jan Jaap Bos (DSEMCO), Hielke Hijmans (Ministry of Justice), Frank van Ommeren (Ministry of Justice), P.M. van Rooijen (ABN AMRO), Prof. J.M. Smits (University of Eindhoven), and René Struik (Philips Crypto).

Last but not least, we are thankful to Vivian Carter for making linguistic corrections.

Babette Aalberts
Simone van der Hof
Tilburg, November 1999

Contents

Digital Signature Blindness

Analysis of legislative approaches to electronic authentication

Babette Aalberts
Simone van der Hof

1. The Context

1.1 Introduction

The need for electronic alternatives to hand-written signatures is increasing with the rise of electronic commerce. For the purposes of this study, electronic commerce (E-commerce) is perceived as *doing business over the Internet*, but may more generally be understood as *doing business electronically*, for instance by means of EDI, fax, telephone, etc. In the last few years, the Internet has developed from a glorified catalogue with companies advertising their products on a passive web site, into a real marketplace with interactive web sites offering a wide range of products and services, which can be ordered, paid for and sometimes even delivered on-line. The nature of the Internet and its increasingly commercial use has confronted governments, businesses and Internet users in general with a spectrum of legal questions, one of which is the legal validity of electronic or digital signatures. To address or not to address this legal problem is a question legislators world-wide have been asking themselves, many of whom have decided in favour of legislation and issued (draft) laws. The wide variety of divergent legislation was one of the starting points of this research (see Chapter 3).

The research presented here was carried out as part of the Dutch National Programme Information Technology and Law (ITeR) and is a continuation of earlier ITeR research, i.e. *The Legal Status of the Digital Signature* by Van der Hof (1997) and *Writings and Signatures: An outdated concept?* by Huydecoper & Van Esch (1997).[1] The first study presented an inventory of legal developments and practical initiatives with respect to digital signatures in some of the European

[1] Van der Hof (1997) Huydecoper & Van Esch (1997) Neither of these studies is available in English, but of the first study a summary in English is on-line available at: <http://cwis.kub.nl/~frw/people/hof/ds-summ.htm>.

Union Member States. The second study explored the functions of writings and signatures as they were intended by the legislator, and evaluated the feasibility of these functions in situations where electronic alternatives to writings and signatures are used. The authors *inter alia* designed a three-prong test (functional-analysis test) to determine the feasibility of electronic-signature techniques to fulfil signature requirements in legislation. In this test, firstly, the legislative considerations for requiring a signature with respect to particular legal actions must be determined. Secondly, functions and characteristics of signatures, which were considered necessary in order to incorporate signature requirements in legislation, should be identified. Finally, the possibility of performing the same functions by applying electronic signatures must be explored. An affirmative outcome of the third prong would mean that the electronic signature is an adequate substitute for the hand-written signature. The functional-analysis test was a second starting point for the present research (see Chapter 4).

1.2 A veritable tower of Babel

As a meticulous reader will have noted, the previous section mentioned electronic signatures and digital signatures. The two concepts should, however, not be confused, in the sense that, although a digital signature is an electronic signature, the latter is a much broader concept than the former. **Electronic signature** includes all technologies for replacing hand-written signatures in an electronic environment, examples of which are the scanned signature, the signature by means of a digital pen and the PIN-code. **Digital signature** is a name for technological applications using asymmetric cryptography, also referred to as public-key encryption systems, to ensure the authenticity of electronic messages and guarantee the integrity of the contents of these messages.[2] The digital signature has many different appearances, such as fail-stop digital signatures, blind signatures and undeniable digital signatures (see table 1).[3] The digital signature is a technology for signing electronic documents electronically, thus, it is an electronic signature, though of a particular kind. The co-existence of these concepts has caused an unfortunate confusion with sweeping consequences.

The confusion started with (from a lawyer's viewpoint) erroneously calling the application of asymmetric cryptography for authentication purposes a digital

[2] For further reading on the technical details of digital signatures and asymmetric encryption: Baum & Ford (1997).

[3] Schneier (1996), p. 34-44, 81-82, 85 and 112-115.

signature. It is, in fact, not a signature in a legal sense at all, though it can be used for signing electronic documents.[4] The digital signature can, as stated earlier, verify the authenticity of electronic messages and guarantee the integrity of the contents. Thus, it does not merely establish origin or integrity with respect to individuals as is required for signing purposes, but it can also authenticate, for instance, servers, web sites, computer software, or any other data that is distributed or stored digitally.[5] Digital signatures, therefore, have a much broader use than an electronic alternative for hand-written signatures. Often, however, this is not sufficiently recognised.

Dumortier & Van Eecke mentioned the example of the Belgian draft law on digital signatures, which should, according to some people, allow legal persons to sign documents. The underlying idea was the fact that web sites often belong to legal persons and legal persons should, therefore, be able to sign. However, there is a difference, which was not recognised by this proposal's proponents, between using the digital-signature technology to stimulate the development of e-commerce and the legal consequences of digitally signing an electronic document. Whereas legal persons should be allowed to do the former, it is not obvious that their actually signing a document will have these legal consequences. As Dumortier & Van Eecke stated, the question of allowing legal persons to sign is of a significantly different nature and is not specifically linked to the use of *digital* signatures.[6]

One option for dealing with the terminological confusion is to change the name by calling it, for example, a digital seal or digital envelope. But 'digital signature' is nowadays so commonly used that it seems impossible to rename the technology. It is important though, to be precise in publications such as this about the exact meaning of the term, the differences with the broader 'electronic signature', and the various possible applications of the technology. Hopefully, awareness of the issue and its adverse consequences (i.e. confusion and non-perspicuous discussions) will lead to a more careful use of the term.

---

[4] This is however not to say that it is an effective means of signing legally in every instance. Whereas digital signatures may provide for authentification of electronic messages, other functions (see 4.2.) may be more problematic. A more appropriate perception of digital signatures may be that of digital *envelopes*, because there is no relation with contents of the signed document. The signer does not have to or will in some instances (in case of e.g. blind signatures) not be able to view the contents of the electronic document to digitally sign it.

[5] From a technical perspective the term signature is understood as any technology which links an entity with data, whereas from a legal perspective a signature is merely the link between a person and data (i.e. a document).

[6] Dumortier & Van Eecke (1999a), p. 3-10. See also Kuner (1998), p. 715, discussing the situation in Civil Law countries where only a natural person can sign, which limitation does not exist under Common Law.

Electronic signature	Every way of authenticating data by means of information technology		
Example of electronic signature	**Digital signature**	Protocols based on asymmetric encryption, which can ensure the authenticity and integrity of electronic data.	
	Examples of digital signatures	**Blind signature**	Digital signature protocol, which allows a person to sign a document without knowledge of the contents of the document.
		Fail-stop digital signature	Digital signature protocol, which allows a signature-holder to prove that a digital signature forged after a brute force attack is a fake.
		Proxy signature	Digital signature protocol, which allows the signer to give authority to sign a message to someone else, without disclosing his/her private key.
		Undeniable digital signature	Digital signature protocol, which cannot be verified without the signer's consent (to prevent e.g. exact copying of digital signatures). Designated confirmer signatures allow others than the signer to verify the signer's signature.

Table 1: Definitions of electronic and digital signatures[7]

1.3 Legislative chaos

In addition to, and partly as a consequence of the terminological confusion, electronic and digital signatures as well as related topics, such as Certification Authorities,[8] Public-Key Infrastructures,[9] are the subject of many, quite different laws or regulations world-wide.

As stated, the legislative chaos is partly a result of the terminological shambles. Depending on the application of the digital-signature technology, i.e. general use to ensure the reliability of transactions or specific use for signing purposes to fulfil formal requirements, the legislator has focussed upon, the subject of legislation is (on a sliding scale) more technically or more legally oriented. The

[7] These definitions are based on Schneier (1996), supra note 3.

[8] A Certification Authority (CA) is a trusted third party (TTP), which certifies public keys, publishes certificates and revokes certificates.

[9] A Public-Key Infrastructure (PKI) is a hierarchic or horizontal structure of CAs, which are subjected to the same organisational, technical and procedural rules and which may (cross-) certify each other.

technical approach, at one end of the scale, means recognising the digital-signature technology as a standard for secure electronic commerce and is mainly concerned with the general use of the digital-signature technology. The legal approach, at the other end of the scale, encompasses the legal equation of hand-written and electronic or digital signatures and, thus, aims at the digital signature for signing purposes. To complicate matters even more, between these extremes, legislation with combined technical and legal approaches can be identified, which, e.g., focus on a certain technology, such as digital signatures, that is considered adequate for legally signing electronic documents. Within the legal and technical approaches to regulating digital signatures, the methods of approach may differ as well. For example, in equating traditional and electronic signatures, some laws specify an open approach, merely providing that electronic signatures will not be exempted from legal effect, whereas other laws impose the aforementioned functional-analysis test to specific legal provisions. The sum of all these differences is legislative chaos.

Another complicating factor in electronic and digital-signature legislation is that often requirements of form are not dealt with in one legislative instrument. In other words, electronic or digital signature legislation does not consistently address writings, signatures and other formal requirements, but in some countries merely addresses the signature as such.

From a legal and combined technical-legal perspective, this is an unfortunate development, since both requirements are bound to each other and need to be addressed coherently in order to achieve legal certainty in, for instance, matters of enforceability of legal actions and evidentiary matters. From a purely technical perspective, which is, as mentioned earlier, concerned with stimulating the general use of digital signatures to achieve reliability in electronic commerce, this approach seems less troublesome, since it is concerned with the technology as such and not with legal requirements of form. However, this is only true insofar as these technical regulations do not have any (implicit) legal implications.

The consequence of this legislative chaos is that electronic or digital-signature legislation seems to achieve the opposite, namely, legal insecurity and unpredictability in electronic commerce. The co-existence of these many, mutually exclusive (national or local) laws and regulations may seriously impede the smooth development of a truly international phenomenon such as electronic commerce. It is true that international organisations such as the United Nations Commission on International Trade Law (UNCITRAL) try to co-ordinate these efforts by issuing, e.g., model laws. These honourable initiatives have, however, produced only a still too limited effect.

1.4 Definition of research

The main aim of this research is to provide recommendations to the legislator when addressing legal requirements of form in legislation. This objective is encapsulated in the following research question:

Which considerations should be taken into account, if the legislator addresses the subject matter of legal requirements of form in the light of ICT developments?

In order to formulate these recommendations, it is necessary to further outline the context of electronic authentication and the regulatory environment within which this issue is addressed as well as the approaches already taken by national and international regulators.

Chapter 2 sets off with some general topics, which are important to put the issue of electronic authentication regulation in perspective. These topics are:
1. The attraction of the digital signature,
2. Technology neutrality versus technology dependence,
3. National versus international approaches,
4. Civil law versus common law perspective,
5. Government regulation versus self-regulation.

In **Chapter 3**, the approaches towards electronic-authentication legislation and regulations are identified and analysed. Of each approach, several examples are presented and evaluated with respect to each other. These approaches are:
1. The digital signature approach,
2. The two-prong approach, and
3. The minimalist approach.

At the end of this chapter we have presented a synthesis of these approaches in pursuance of which interim conclusions are drawn. In these interim conclusions, we have given preference to the minimalist approach.

Chapter 4 further explores the principle of minimalism by focussing on the functionalist approach. Within the minimalist approach, we have distinguished between the specific-functionalist approach and the generic-functionalist approach. In order to allow for some fine-tuning, both approaches will be further elaborated. In the end we have again shown a preference for one of the approaches, i.e. the generic-functionalist approach.

On the basis of the previous chapters, **Chapter 5** finally formulates the results of this research as recommendations to the legislator on how to handle legal requirements of form when adjusting legislation to the digital environment.

2. General overture

Before we explore the approaches, which can be identified with respect to electronic-authentication legislation, some general considerations are necessary to put the matter into perspective:

(1) The attraction of the digital signature.
(2) Technology neutrality versus technology dependence.
(3) National versus international approaches.
(4) Civil law versus common law perspective.
(5) Regulation versus self-regulation.

2.1 The attraction of the digital signature

The digital signature, and asymmetric-encryption technology in general, is an important technology from the viewpoint of secure electronic commerce. Several applications have been developed using asymmetric encryption to transmit data securely over the Internet, such as SET (Secure Electronic Transactions),[10] SSL (Secure Sockets Layer)[11] and PGP (Pretty Good Privacy).[12]

A digital signature is a document-dependent way of encrypting data by applying asymmetric encryption. Asymmetric encryption uses a key pair, consisting of a private and a public key. To digitally sign a document, first, a hash value must be created. A hash value (also: hash or message digest) is the result of a mathematical calculation (using algorithms also called hash functions), which transforms the document into a string of a certain length. The hash value is, subsequently, signed by the signer s private key and added to the document. The

10 SET is a cryptographic protocol, developed by Visa and Mastercard, for making secure bankcard payments over the Internet.

11 SSL is a cryptographic protocol for sending data, such as credit-card data and bank-account numbers, securely via the Word Wide Web. Websites URLs, which are protected by SSL, start with 'https' instead of 'http'.

12 PGP is a software program for encrypting electronic data, most notably e-mail messages.

addressee can check the (supposed) origin of the document by applying the signer s public key to the digital signature and checking whether the hashes match. The digital signature further ensures the integrity of the document, because the hash value will have changed when the document has been tampered with.[13]

Until now, the digital signature is considered the most adequate means of providing an electronic equivalent to hand-written signatures and, thus, a great deal of the attention is specifically given to this technology. However, apart from the question if the digital signature is legally valuable in every instance,[14] other alternatives to traditional signatures exist as well and rapid ICT developments may in the future lead to new technologies to "sign" electronic documents. A recently developed technique for secure credit card payments (virtual credit acrd (VCC)) does not require a digital signature at all but provides nonetheless a simple and reliable solution for authorising credit card payments over the Internet.[15] All in all, it is important to keep an open mind toward new emerging technologies: every regulatory and legislative initiative should be regarded in the light of new developments.

Moreover it is important to note that technologies may differ as to their reliability and security and not in every instance the highest reliability and security level will be required.[16] There is a tendency of requiring higher levels of reliability than is necessary for the purposes to be served and often policy makers and legislators seem to lose sight of the fact that hand-written signature were never that reliable either, rather on the contrary.[17] Demanding higher

---

13 For further reading on the technical details of digital signatures and asymmetric encryption: Baum & Ford (1997).

14 See Note 4 and Paragraph 4.3.1.3.

15 See Automatiseringsgids, 24 September 1999. VCC is developed by Bernacchi and has already been introduced by the Brazilian bank Unibanco. In this system, the consumer pays by providing a onetime VCC-number to the on-line shop, which he has received by his bank. When the consumer makes a request for a VCC-number, the bank is informed of the transaction and the payee. The bank will pay only once on presentation of the VCC-number and only to the person or company mentioned as payee by the consumer. In this scenario, the consumer does not have to provide his credit card number when making payments over the Internet. The system can be used for virtually any kind of transaction.

16 Apart from technical suitability, economic factors will most certainly play an important role as well, because of the cost effectiveness of applications. We will, however, not further, elaborate on this issue.

17 See also Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996), No. 16: "*[T]he adoption of the functional-equivalent approach should not result in imposing on users of electronic commerce more stringent standards of security (and the related costs) than in a paper-based environment*". Kuner & Miedbrodt (1999), different reliability requirements exist, however, in legal systems. The German legal system, for instance,

reliability requirements merely because it is possible, would be a major (and unjustified) impediment to the development of e-commerce.[18]

2.2 Technology neutrality versus technology dependence

Legislative approaches to new technologies must accommodate the inherent tension between the goal of rendering legislation time resistant and the goal of prescribing specific legal consequences to new technologies, thus, providing legal certainty.[19] Also with respect to electronic authentication legislation the problem of how to deal with the dilemma has presented itself: should legislation be more technology-specific or more technology-neutral?
In the national and international discussions on electronic authentication, the question of whether to regulate certain specific technologies or not is clearly reflected. The different manner in which legislators and policymakers have sought to accommodate the conflicting technology-neutral and technology-specific approaches largely defines the typology of existing approaches toward electronic authentication legislation in theory. Legislation is on a sliding scale more technology-specific or more technology-neutral, which amounts to the contrast of more or less legal security.
As there is another side to every coin, each approach in the debate has its pros and cons. Both the technology-specific and technology-neutral approach have their drawbacks and benefits.

2.2.1 Pros and cons of technology-specific legislation

Some legislators have focussed on specific technologies in their legislation. This kind of legislation may be perceived as originating from specific technological developments. Such a definition would, however, be overly broad and a more appropriate definition is that of legislation, which is based on one or more specific techniques.[20] The extent of the concept of 'technology-specific legislation' is not completely clear.[21] Most technology-specific laws with respect to electronic authentication are, however, based on one technique, namely the digital signature, and not technological developments as such. Legislators and policymakers in favour of technology-specific legislation believe that the continuing expansion of new technologies requires a known and reliable system

sets rather high reliability standards for signatures if compared with the legal system of the United States legal. See also Huls-Report (1998), paragraph 2.5.3.

18 See also UNCITRAL Model Law (1996), No. 16.

19 Baker & Yeo (1999).

20 See also De Cock Buning (1998), p.129

21 Stuyt (1999), p.18.

with established legal consequences. Thus, they prefer to enact legislation, which specifically addresses the use of the digital-signature technique, and to save future issues raised by new techniques for a later date.[22] Technology-specific legislation permits detailed statutory alignment and policymaking in the context of the known capabilities or weaknesses of the particular technology[23] in order to provide the necessary legal security.

The Memorandum *Legislation for the Electronic Highway* from the Dutch Cabinet lists some circumstances, in which technology-specific provisions would be appropriate:

(a) In cases where these provisions define the extent of a regulation,
(b) In cases where legal subjects need insight in a (complicated) technology,[24]
(c) If technology-neutral rules provide insufficient, little or no hold regarding the rights and duties of legal subjects, and
(d) In cases where these provisions are necessary to determine the conditions for government infringement of the legal subjects rights and duties.[25]

Thus, there may be developments, which would make a technology-specific approach recommendable. One of the main benefits is that technology-dependent approaches may lead to more legal security than technology-neutral approaches, which would prevent the courts from having to develop case law on the subject.[26] Some supporters of technology-specific rules even claim that the technology-neutral lobby is mostly based on a myth: neutrality is more of a political buzzword than a clearly defined legal concept.[27] The urge to prescribe legal consequences to certain technologies stems from the experience of certain techniques and their reliability, which renders them feasible for usage in a legal context. Over the last years, this view to legislation, which emanates from technological developments, has resulted in laws specifically regulating digital signatures.

2.2.2 Pros and cons of technology-neutral legislation

The technology-neutral approach refers to legislation, which (under certain conditions) permits the use of *electronic signatures* or even other electronic authentication methods in instances where otherwise a legal requirement of

22 Baker &Yeo (1999).
23 Ford & Baum (1997), p. 296.
24 See also: Arkenbout (1998), p.161.
25 Memorandum Dutch Cabinet (1998), Nos. 1-2, p. 14.
26 See for this example: Beary (1998).
27 Baum (1999).

form could not be met, but does not specify any technique or implementation of a certain technique.[28] Technology-neutral legislation may, thus, give the same legal status to electronically signed documents as to written and signed documents whatever form of electronic signature is used. If necessary, authority to issue more detailed rules on specific matters may then be delegated to the appropriate administrative body.

This approach, which is also referred to as the minimal approach, provides flexibility in the sense that various technical methods, including new techniques that may be developed in the future, can be used to comply with formal requirements. The proponents of technique-neutral legislation are of the opinion that this kind of legislation will be better suited to survive technological changes.[29] Moreover, legislators and policymakers in favour of technology-neutral legislation are concerned that premature endorsement of a particular technology will set them outside the mainstream of technology and legislative initiatives as well as developments internationally.[30]

Presently, the technology-neutral approach to electronic authentication legislation seems to become ever more prominent. New legislative initiatives generally choose a more open approach, which leaves room for new technological developments. One of the reasons is the growing awareness as to the fact that other technologies, such as dynamic signature analysis,[31] are catching up and may soon compete with digital signature technologies or, at least, present another adequate and functional authentication technology in certain situations. The use of different authentication methods must, therefore, not be excluded, since technologies will (be able to) serve different purposes and some technologies will be better suited " to do the job" than others.[32] There will not exist just one technology, which is the most adequate to be applied in every situation.

---

28 Beary (1998).

29 See, e.g., De Cock Buning (1998), p. 134.

30 Baker & Yeo (1999).

31 ILPF Survey (1999). Dynamic-signature analysis uses a digital pen, which records the speed and pressure when signing a document. Examples of dynamic-signature analysis are Penop (<http://www.penop.com>) and Cybersign (<http://www.cybersign.com>).

32 Digital-signature applications, e.g., are not very user-friendly (yet), and, therefore, less suited for consumer transactions.

	Advantages	Disadvantages
Technology-dependent legislation	• Allows for legal certainty • Provides a reliable system with established legal consequences • Prevents the court from having to develop case-law on the subject • Permits detailed statutory alignment and policymaking in the context of the known capabilities weakness of the particular technology	• May soon have to be adjusted • Premature endorsement of a particular technology may set it outside the mainstream of technological developments • May distort the natural market flow • May be superfluous
Technology-independent legislation	• Allows for flexibility • Is not soon outdated • May survive technological changes • Leaves room for new technological developments • Intents to ensure legal equivalence among various new technological approaches	• Allows for legal uncertainty • Is more of a political buzzword than a clearly defined legal concept • Language of neutrality my undermine support for an already proven and available technology • Leaves room for new technology to develop and capture the market

Table 2: Technology-dependent versus technology-independent legislation

2.2.3 Final remarks

The e-commerce market is of a dynamic character where technological developments are going fast, thus, new transaction and payment ways will evolve at a fast pace, using new and different means of authentication.[33] A good example can be found in the field of Internet payment systems. The market expects a high flight from the introduction of the SET (Secure Electronic Transaction) technology, an asymmetric encryption based technology developed jointly by VISA and Mastercard. Meanwhile, however, other payment systems are under construction as well, one of which is iPIN. iPIN enables payment of small Internet transactions via an ISP or telecommunications company by using a PIN-code. The application may be much more consumer-friendly than SET, which in contrast to iPIN requires downloading and installing of software (electronic wallet).[34] At the same time, it is a great opportunity for ISPs and

[33] Dumortier & Van Eecke (1999a), p.5, as a result of rapid changes in the environment of information technology electronic signatures could in the future be produced by other means than the technology of the digital signature. See also Paragraph 2.1.

[34] Information on iPIN is available at <http://www.ipin.com>. Information on SET is on-line available at <http://www.mastercard.com/shoponline/set/set.html>.

telecommunications companies to enter the Internet payment market by serving as intermediaries, since they already have important accounting possibilities in their primary functions. A second example, which seems very promising, has already been mentioned in paragraph 2.1: the Virtual Credit Card (VCC).
The possibilities seem to be infinite and developments to invent ever more innovative, easy-to-use and fast methods for doing business on the Internet are continuing, yet, the direction in which these developments will go is often unpredictable. In our opinion, it is important not to impede these developments by issuing premature legislation, which distorts rather than stimulates the market.[35] A more technology-neutral approach will most likely be better suited to deal with future technologies than legislation that focuses solely on a specific technology.

2.3 National versus international

National and international legislative initiatives with respect to electronic authentication are often lumped together. For the purpose of the question raised in this study of how to address electronic authentication legally, it is important to differentiate between the different levels.
International approaches to electronic authentication are quickly gaining importance and even seem to outstrip national initiatives as a result of the inherent international character of the Internet and, thus, of electronic commerce. The international nature of the Internet requires an international approach toward regulatory matters in order to ensure world-wide legal predictability.
However, in the short term uniform international legislation will in many instances be a utopia rather than an ideal within reach. The cultural and legal differences among countries world-wide are too much of a barrier for quick resolution of the many legal issues raised by electronic commerce, one of which is electronic authentication.
For this reason, it is of the utmost importance that national governments put their legislation in order, if they intend to stay in the running called e-commerce. As regards the requirements of form, national legislators will have to analyse and evaluate their national legislation in order to get rid of outdated concepts or adjust them to fit the electronic environment. By doing so, they should, however, act in line with international developments and avoid as much as possible acting on their own initiative: they should think internationally rather than at all costs adhering to their own legal concepts.

35 See Biddle (1997).

National legislation is or can be concerned with matters in a much more concrete and detailed way, whereas international initiatives in the short run better deal with the issue in a more abstract and open way in order to be widely acceptable. An exception is the European Union, which aims at harmonising *national* legislation and, therefore, may be considered more of a national character rather than being a truly international initiative. Nevertheless, both the (Draft) Electronic Signatures Directive and the Draft E-Commerce Directive (see 3.2.2.2.) are interesting measures from an international perspective, since both directives aim at aligning the differing national legislations in order to facilitate and stimulate the *European* market. It is "just" one step further to do the same for the *international* market.

2.4 Common Law versus Civil Law

Kuner & Miedbrodt write:

"While there has been considerable regulatory activity concerning electronic signatures in recent years in a number of countries, so far a lack of understanding about the differing roles of signatures and written form in different legal systems has contributed to difficulties implementing internationally-acceptable rules for electronic signatures."[36]

As regards these "*differing roles*", Kuner & Miedbrodt refer to the differences between Common Law and Civil Law.[37]

Kuner & Miedbrodt identify major differences between Common Law and Civil Law with respect to the meaning of requirements of form. In the United States, for instance, the emphasis is on the signer s intention to be bound, rather than on the security of the signing process.[38] As an additional requirement, the signature must be recorded on a tangible medium. If these factors are satisfied, a signature will be considered legally valid. Furthermore, Kuner & Miedbrodt say that in the United States formal requirements have largely decreased in significance.[39]

---

36 Kuner & Miedbrodt (1999), p. 144.

37 See also Kuner (1998), p. 714.

38 Putting one's X or mark on a document will be considered a signature in Anglo-American countries but not in, e.g., the Netherlands, Huydecoper & Van Esch (1997), p. 116.

39 Kuner & Miedbrodt (1999), p. 146 and 150. In the United States, the Drafting Committee on the Uniform Commercial Code (UCC) is considering to repeal the Statute of Frauds with respect to the sale of goods, Baum & Ford (1997), p. 44. Information on the UCC Draft Revisions is available at:

The question rises, why so many electronic authentication laws have been issued or are pending in the USA. According to Kuner & Miedbrodt, this has not so much to do with the admissibility of electronic signatures as such, as with legal insecurity surrounding the evidentiary status of electronic signatures.[40]

In contrast, as an example of a Civil Law system, German legal requirements of form cannot be moulded as liberally as in the U.S. situation, which amounts to the need for a high level of reliability and security in order to satisfy these requirements.[41] For instance, written documents must be personally signed and stamps, typewritten or faxed signatures are not considered personally signed.[42] If a document is appropriately, i.e. manually, signed, it has an enhanced evidentiary status, meaning the signed declaration is presumed to originate from the signer. An electronic document cannot have this status, since it cannot be manually signed. However, electronic documents may still be presented as visual or expert evidence.[43]
The heavy requirements set by German law explain the choice for a digital signature law, setting the secure digital-signature technique as a standard and at the same time establishing a security infrastructure (see paragraph 3.2.1.1.).

Different concepts of writings and signatures will have an influence on the development of national electronic-authentication legislation and these laws should, therefore, be contemplated against the background of the legal system concerned to fully grasp their meaning.

2.5 Government regulation versus self-regulation?

The different regulatory initiatives in the field of electronic authentication can be qualified as government regulation, industry self-regulation or a mixture of both, which is called co-regulation.

The majority of the regulatory initiatives in the field of electronic authentication fall under the category of government regulation. Governments are adjusting

---

<http://www.law.upenn.edu/library/ulc/ulc.htm>.

40 Kuner & Miedbrodt (1999), p. 146.

41 See also the German Government Position Paper on the International Recognition of Digital Signatures, available at:
<http://www.kuner.com/data/sig/gov_digsig_recognition.html>
and Schulzki-Haddouti (1999).

42 In the Netherlands, however, a signature by facsimile is allowed. Because of the requirement that a signature must show a person's handwriting, typewritten signatures and stamps using printed letters are not allowed. Huydecoper & Van Esch (1997), p. 116.

43 Kuner & Miedbrodt (1999), p. 146-149.

existing legislation or issue new legislation to accommodate the digital era. In cases where, e.g., requirements of form are fundamental requirements for the validity of legal acts, such as contracts, and the admissibility as evidence or the evidential value of electronic documents is at issue, government intervention may well be necessary to resolve legal uncertainty. In many instances legal provisions in this respect will be of a mandatory nature, meaning that they cannot be set aside via contracts. Self-regulation is then less or not suitable for resolving legal uncertainty, unless governments were to be involved as well (co-regulation).

Some initiatives can be classified as industry self-regulation, which is sometimes also referred to as soft law or best practices. Especially in an area that experiences rapid technological changes, such as e-commerce, self-regulation can be an important means of regulation due to its flexibility and practical as well as realistic nature.
Industry self-regulation may appear in different forms, for instance, self-regulation by setting a technical standard or self-regulation by putting forward basic legal principles. An example of the technical standard self-regulatory approach is, for instance, the work of the PKIX Working Group of the Internet Engineering Task Force (IETF).[44] In 1995, the Working Group was established with the intention to develop Internet standards needed to support a PKI on X.509 certificates.[45] Part of its work is dedicated to developing certification protocols for use in legal contexts, such as so-called qualified certificates.
The self-regulatory approach based on basic legal principles was, e.g., put forward by the Internet Law & Policy Forum (ILPF).[46] ILPF is an international forum of market parties, which amongst others develops principles and policies for global use to accelerate the growth of electronic commerce and Internet transactions. The Digital Signature Working Group has drafted a set of legislative principles for electronic authentication, which "are intended to facilitate the creation of a predictable legal environment for electronic commerce based on recognition of electronic authentication of signatures and records."[47] The approach taken by ILPF is technology-neutral and market-driven.

Another approach to regulation is when private sector and government join forces and share the regulatory role. This is called co-regulation. Co-regulation goes further than what is called conditioned self-regulation, where governments set a framework for further elaboration by the private sector. Examples of co-

44 See <http://www.ietf.org>.

45 Public-Key Infrastructure (X.509) (pkix), 29 September 1999, <http://www.ietf.cnri.reston.va.us/html.charters/pkix-charter.html>.

46 See <http://www.ilpf.org>.

47 See <http://www.ilpf.org/digsig/principles.htm>.

regulation are codes of practice developed by industry in consultation with the government.[48] For instance, the Electronic Commerce Platform in the Netherlands (ECP.NL) has drafted a Code of Conduct for Electronic Commerce and is at the same time involved in the TTP.NL project.[49] Both the Code and the TTP.NL project involve consultation between industry, government and interest groups (e.g. the Consumer Association).[50] Another illustration of this approach is the Code of Practice[51] drafted by the Australian Internet Industry Association (IIA).[52] The Code of Practice is a result of ongoing consultations with the Australian government, industry and consumer groups.

Each of the aforementioned regulatory approaches has to be valued properly. Self-regulation is advocated strongly where Internet regulation is concerned for various reasons. First, self-regulation allows for flexibly anticipating technological developments. Second, industry and user groups will in some instances be better capable of generating (legal) solutions. Finally, self-regulation is not confined to geographical borders.[53]
Government regulation, on the other hand, is characterised as inflexible, national, slow and obsolete before even being operational and not always realistic where market and technological developments are concerned.[54] However, in some areas government regulation is important, because fundamental standards are concerned, e.g., fundamental rights (such as privacy protection), consumer protection and law enforcement. Ideally, governments should attempt to approach these fundamental issues internationally, however, this will not always be easy due to cultural differences between countries.
Co-regulation is a way of balancing government regulation and self-regulation and, thus, profiting of advantages on either side.[55] Both the legislative powers of the government and the involvement of industry in fashioning the legal environment of e-commerce are respected. With both co-regulation and conditioned self-regulation the importance of fundamental standards can be

48 Australia (1997).
49 See <http://www.ecp.nl>. On the Code of Conduct for Electronic Commerce see: The EDI Law Review 6: 73-122, 1999.
50 See for information on both projects <http://www.ecp.nl/vertrouwen/> (in Dutch). Code of Conduct for electronic commerce, Draft version 2.0, <http://www.ecp.nl/vertrouwen/Ecode2-0.zip>.
51 See <http://www.iia.net.au/code.html>.
52 See <http://www.iia.net.au/>.
53 Heineman (1999), p. 153.
54 See, for instance, ILPF report (1998).
55 It seems likely that cultural differences may have an impact on the possibility and effectiveness of co-regulation. It is, for instance, important that the government is trusted sufficiently to be regarded as a valuable partner by industry and other interest groups.

respected and at the same time there is the advantage of the flexibility of self-regulation mechanisms.

As regards electronic authentication the emphasis is still largely on government regulation, although some self-regulation or co-regulation initiatives unfolded as well (e.g. ILPF Principles, ECP.NL Code of Conduct and TTP.NL). Since electronic authentication is a technologically dynamic field with need for a flexible and international approach on the one hand, but on the other hand affects fundamental standards in most legal systems, perhaps a more combined approach should be opted for. Electronic authentication is a complex matter and much of the knowledge concerning techniques involved as well as market and technological developments is to be found in the business and research field rather than with government officials. It is, therefore, of great importance that these experts are involved in the regulatory process. These developments, furthermore, should not be hampered by premature and unrealistic government regulation. Moreover, electronic commerce, electronic authentication being a part of that, raises cross-border issues, which should ideally be dealt with from an international perspective. At the same time, electronic authentication raises some fundamental questions, which ask for direct government regulation. For one thing, legal requirements of form cannot always be circumvented by contract and need to be addressed by the government. The implementation of biometrics also raises questions of a fundamental nature.[56]
All in all, both self-regulation and government regulation are relevant tools to deal with electronic authentication. Ideally, industry should be in close consultation with the government when drafting self-regulation (co-regulation) and the government should work closely together with technology and market experts when adapting legislation to electronic commerce. How to shift the focus that is now mainly on government regulation more in the direction of self-regulation and co-regulation is still a matter for further consideration and research.

[56] See, e.g. Van Kralingen, Prins & Grijpink (1997), p. 23-39, on biometrics in relation to fundamental rights.

3. Approaches in electronic authentication legislation

3.1 Introduction

Requirements for electronic authentication have already been set forth in numerous regulatory initiatives and legislative measures in order to provide legal security and encourage the use of these technologies for electronic commerce purposes. On an international level, the United Nations Commission on International Trade Law (UNCITRAL), the International Chamber of Commerce (ICC), and the Organisation for Economic Co-operation and Development (OECD) have released, or are working on, rules with respect to electronic authentication. In Europe, the European Union (EU) and several countries, such as Germany and Italy have issued (draft) legislation. The same is true for many U.S. States, for countries in Asia (Malaysia, Singapore) and South America (Argentina, Columbia), and Australia.[57]

This chapter aims to shed light on the recent developments in electronic and digital-signature legislation approaches. We will identify, illustrate and analyse different approaches in electronic authentication regulatory initiatives.

3.2 Legislative approaches toward electronic authentication

Classifying the existing legislation with respect to electronic authentication is not an easy task on account of the many differences that exist. It is, however, possible to sketch the main approaches at a national and international level.

[57] Digital Signature Law Survey (1999). See also ILPF: Digital Signature Working Group, <http://www.ilpf.org/digsig/digsig.htm>.

Three approaches can be identified:
1) The *digital signature approach*
2) The *two-prong approach*
3) The *minimalist approach*

3.2.1 The digital signature approach

The digital signature approach is characterised by its focus on the digital signature technique. Legislation under this category is truly *digital signature* legislation because it regulates (on the basis of) digital signatures. Digital signature legislation is technology-specific legislation by definition.

Legislation under the digital signature approach is solely concerned with the (evidentiary) status of the *digital* signature. The digital signature approach knows three variations, which we have distinguished as follows:

1) The technical variant
2) The legal variant
3) The organisational variant

3.2.1.1 Technical variant

The technical approach amounts to setting the digital signature technique as a technical standard by means of a legal instrument. The technical approach does not deal with legal consequences, although such consequences may implicitly follow from the use of digital signatures in accordance with the law concerned.

An illustration of the technical variant is the German Digital Signature Law. Germany was one of the first countries in the world to enact a comprehensive digital signature law with special technical requirements for a system where security is based upon a PKI infrastructure.[58] The aim of the German legislator as regards the digital signature law was to provide a safe and secure infrastructure for the use of signatures in order to let electronic commerce flourish.
The requirements for the digital signature standard are determined in the Signature Ordinance (*Signaturverordnung*) and a Technical Catalogue (*Massnahmenkatalog*).[59] The standard will cover the technology of the digital signature, but simply and solely as far as the authentication function is concerned. Other functions do not fall under the technical standard. Moreover,

[58] Kuner (1998), p.712.
[59] Roßnagel (1997), p.75.

no explicit legal consequences derive from the German law as regards the use of this standard. [60]
The question is whether Germany s trailblazer role will yield an inspiring model. According to Dumortier & Van Eecke, the German government has caused total confusion by using a legal instrument to set a technical standard.[61] The digital signature law establishes a security standard for the specific digital signature technique. The German government should rather have left the establishment of a standard to the appropriate organisations, such as the Bundesamt für Informationssicherheit (Federal Agency for Information Security).[62] Moreover, the digital signature law is not imperative law and digital signatures will not be legally recognised even if the law would be imperative.
The heavy requirements set by the German law are a drawback, which may cause Germany to fall behind rather than make their anticipated pioneering role as far as e-commerce is concerned come true. These requirements are a direct result of the high reliability requirements set by German legislation with respect to legal requirements of form (see 2.4).[63]

3.2.1.2 Legal variant

The legal variant of the digital-signature approach is found in legislation, which specifically regulates digital signatures in order to provide this technique with a legal status similar to that of the hand-written signature. The general purpose of these laws is to provide legal security for the use of digital signatures. Often legislation of this kind also includes the implementation and regulation of a Public Key Infrastructure (PKI). In the next sections, two examples of the legal variant will be presented:
1) the Utah Digital Signature Act, and
2) the Italian Digital Document Regulations.

3.2.1.2.1 Utah

A Common Law example of the legal variant of the digital signature approach is the Utah Digital Signature Act of 1995, which aims at facilitating the digital-

60 The German Ministry of Justice is, however, in the process of examining existing laws in order to improve the legal status of electronic signatures. See also Entwurf eines Gesetzes über den Elektronischen Rechtsverkehr, (Draft law on electronic judicial matters),Bundesnotarkammer, 29 April 1998, on-line available at: < http://www.bnotk.de/geselrev.htm>.

61 Dumortier (1998), p. 2-3. Another example of a government technical standard is the US Digital Signature Standard (DDS), <http://www.epic.org/crypto/dss/>, which has however not been put forward by means of legislation.

62 Dumortier & Van Eecke (1999a), p. 6.

63 See also Schulzki-Haddouti (1999).

signature technique through detailed regulations.[64] The Utah Act sets rules, which seem to have a technology-neutral character at first sight. However, it actually deals with asymmetric cryptography and maintains existing legislation addressing signatures, such as requirements of form, as much as possible. Due to the fact that the Utah Digital Signature Act is very explicit about the digital signature technology by specifically regulating signatures based upon asymmetric encryption, it is also known as "thick" law.[65] Under the Utah Act, a digital signature will have the same legal effect as a hand-written signature, under the condition that all the requirements in the Act are met.
According to Van Esch, the Utah Act insufficiently takes into account the various functions of the signature, which often form the basis for legal requirements of form.[66] However, as mentioned before one must take into account the legal system from which legislation originates. Utah is a Common Law system, which generally has more liberal requirements for the use of signatures. Expressing one s intention on a particular matter, electronically or otherwise, may be sufficient to assume that a person has "signed". The admissibility of electronic signatures as evidence in court, however, poses problems, which is the main reason for U.S. governments to issue legislation (see 2.4.). Distinguishing between the (other) functions of requirements of form is, therefore, less obvious here than in Civil Law systems.

3.2.1.2.2 Italy

A Civil Law example of the legal variant of the digital signature approach is the Italian Digital Document Regulations of 10 November 1997 (Presidential Decree No.513). The regulations elaborate on article 15 of Law No. 59 of 15 March 1997, which deals with the simplification of public administration. Article 15 allows the use electronic documents in public administration. Moreover, technical rules for digital signatures have been adopted in April 1999, which further implement Law No. 59 by, amongst others, prescribing the techniques to be used and determining obligations of key holders and CAs.[67]
The Digital Document Regulations provide legal recognition of digital documents, digital signatures, digital contracts and digital payments. With respect to signatures, digital signatures can under certain conditions be used as an equivalent to hand-written signatures, seals, embossing, stamps, signs and marks of any kind. These conditions include the use of certification services by a CA. The requirements, which companies have to fulfil in order to become a CA

64 Utah Digital Signature Act (Utah Code §§ 46-3-101 et seq. (1996) <http://www.commerce.state.ut.us/web/commerce/digsig/act.htm>.
65 Tikwart (1998).
66 Van Esch (1999), p.190.
67 Digital Signature Law Survey (1999).

are very strict, in the sense that only joint-stock companies with large capital (comparable to companies in the financial sector) are allowed to provide these services.[68]
Italian legislation on electronic authentication clearly illustrates the technology-specific way of dealing with legal requirements of form.[69] The regulations put forward the PKI system and are limited to public-key cryptography, i.e., digital signatures.[70]

3.2.1.3 Organisational variant

The organisational variant of the digital signature approach, neither sets the digital signature as a technical standard nor provides for explicit legal recognition of the digital signature, but addresses the organisation of CAs and the use of digital certificates in connection with digital signature applications. The aim is to promote trust and reliability in electronic transactions by ensuring that CAs are reliable and secure.

One example of this variant is the CA-guidelines in Japan, which have been issued by the CA Working Group of the Electronic Commerce Promotion Council of Japan.[71] The Guidelines present guidance to companies, which operate as a CA, by providing detailed management requirements, operation requirements, and system and facility requirements. The Guidelines focus primarily on open user groups, but may also provide guidance for closed systems.

Another example is the Dutch National TTP Project, which will amount to preconditions for the commercial exploitation of Trusted Third Parties in the Netherlands. At present, the implementation of the EU Directive on Electronic Signatures (see paragraph 3.2.2.2) is anticipated under the TTP.NL framework.

3.2.1.4 Synthesis

All of the initiatives under the digital signature approach are of a national character and, with the exception of the Italian legislation, they are all early regulations. Along with their focus on digital signatures, these regulations aim at the establishment of Public Key Infrastructure in order to ensure, *inter alia*, that the digital signature can fulfil its identification and authentication functions in a reliable way. This is, however, as far as the similarity goes, for the binding character as well as the goal and effects of these initiatives differ.

---

68 Digital Signature Law Survey (1999).
69 Cerina (1998), p.193-9.
70 IVIR (1998), p. 23.
71 CA Guidelines, Version 1.0, <http://ecom.ecom.or.jp/ecom_e/cag-smry.htm>.

The German, Italian and Utah Act are "real" legislation and have a binding effect upon parties concerned (hard law), whereas the Japanese guidelines and the framework of TTP.NL merely provide guidance to companies (soft law).
The objective and, therefore, the effect of the examples provided differ in that the German and Japanese regulations as well as TTP.NL, unlike the Italian and Utah laws, do not (explicitly) provide legal consequences regarding the use of digital signatures.[72] Compared to its Italian and Utah counterparts, the German law is, therefore, a strange kind of legislation in that a legal instrument is used to set technical standards and legal consequences are left to be dealt with at a later stage.
The similarity between the Utah and Italian approaches is strange from the viewpoint that Utah has a Common Law system whereas Italy is Civil Law country. The legal variant of the digital signature approach seems more appropriate for Common Law systems than for Civil Law systems, since it merely deals with the evidentiary function of signatures and does not take into account the other functions (e.g., protection of weaker parties) a signature may serve as well. From the point of view of guaranteeing high reliability, which was an important consideration of the German legislator, it is, however, not surprising that the Italian legislator has chosen the digital signature approach. In the light of more recent legislative initiatives, this approach seems, however, to be outdated.

3.2.2 The two-prong approach

The second approach is called the two-prong approach, because of its hybrid way of dealing with electronic authentication. In this approach, legislators aim at making their legislation more time-resistant by, on the one hand, addressing certain technological requirements in their legislation and, on the other hand, by leaving room for new technological developments. With this approach, legislation sets requirements for electronic authentication methods, which will receive a certain minimum legal status (minimum prong) and assigns greater legal effect to certain electronic-authentication techniques (maximum prong). The technologies assigned with this higher legal status are referred to as secure electronic signatures.

The maximum prong is similar to the way the digital signature approach in its second variation (rendering legal effect to the use digital signatures) is dealing with the signature issue. Both the digital-signature and the maximum prong of the two-prong approach set detailed regulations addressing, e.g., the rights and

[72] This may however be different for TTP.NL, if the EU E-signatures Directive is actually going to be implemented within the TTP.NL framework (see paragraph 3.2.1.3).

duties of parties concerned and liability allocation between these parties as well as requiring the establishment of a PKI. In contrast with the digital-signature approach, the two-prong approach does not specify one technology (the digital signature) but leaves room for future technologies to comply with the extra requirements as well. At present, however, solely the digital-signature technique will be protected under the maximum prong.
The minimum prong is similar to the minimalist approach (see 3.2.3.) and by definition leaves room for new technological developments.

In order to illustrate this approach, we will elaborate on three examples:
1) The UNCITRAL Draft Uniform Rules on Electronic Signatures (section 3.2.2.1)
2) The 1999 EU Directive on Electronic Signatures (section 3.2.2.2)
3) The 1998 Singapore Electronic Transactions Act (section 3.2.2.3)

3.2.2.1 UNCITRAL

On the international level the two-prong approach has been introduced in the UNCITRAL Draft Uniform Rules on Electronic Signatures.[73] The Uniform Rules, when adopted, are not binding legislation, but give guidance to governments and legislative authorities that are preparing legislation on electronic signature issues.
The Uniform Rules have been drafted by the UNCITRAL Working Group on Electronic Commerce from the point of view that harmonisation of the law in the field of digital signatures and closely related matters (e.g., PKI) is necessary. At the same time, the Uniform Rules "should be consistent with the media-neutral approach taken in the UNCITRAL Model Law on Electronic Commerce" (see 3.2.3.1.) and "not discourage the use of other authentication techniques."[74]

The Working Group seems to perceive the Uniform Rules as an intermediate phase, for it has expressed the intention to "develop a fully media-neutral rule at a later stage" with respect to the PKI-model.[75] For the time being, the Uniform Rules will, however, focus on currently used (or rather known) technology, such as digital signatures and PKI. To still leave room for new developments and in order not to detract from its technology-neutrality aim, the Working Group has explicitly included a reference to article 7 of the UNCITRAL Model Law on

73 UNCITRAL Draft Uniform Rules (1999).
74 UNCITRAL Draft Uniform Rules (1999), p. 2, No. 3.
75 UNCITRAL Draft Uniform Rules (1999), p. 4, No. 8.

Electronic Commerce.[76] Both regulations, however, constitute separate legal instruments.[77]

Under the current version of the Draft Uniform Rules, electronic signature is defined as:

"[Data in electronic form in, affixed to, or logically associated with a data message and] [any method in relation to a data message] that may be used to identify the signature holder in relation to a data message and indicate the signature holder's approval of the information contained in the data message".

Enhanced electronic signature means:

"Electronic signature in respect of which it can be shown, through the use of [security procedure] [method], that the signature:
(i) is unique to the signature holder [for the purpose for] [within the context in] which it is used;
(ii) was created and affixed to the data message by the signature holder or using a means under the sole control of the signature holder [and not by any other person];
(iii) [was created and is linked to the data message to which it relates in a manner which provides reliable assurance as to the integrity of the message]".[78]

The draft does not provide a definition of digital signature as such, but it seems clear from the above-cited text that the concept is included in the definition of enhanced electronic signature (see under (iii)).
The Draft Uniform Rules provide that where an enhanced electronic signature is used, there is a presumption that the data message is legally signed.

3.2.2.2 EU

Another illustration of the two-prong approach is the Directive of the European Parliament and of the Council on a Common Framework for Electronic Signatures.[79] The Directive was drafted for the purpose of creating a

---

76 Article 2 of the Draft Uniform Rules states: "The provisions of these Rules shall not be applied so as to exclude, restrict, or deprive of legal effect any method [of signature] that satisfies the requirements of [article 7 of the UNCITRAL Model Law on Electronic Commerce]". See further: article 6 and 7 of the Draft Uniform Rules.

77 UNCITRAL Draft Uniform Rules (1999), p. 5, No. 16.

78 The brackets indicate changes from earlier versions or issues, which are still under discussion, see Remarks, UNCITRAL Draft Uniform Rules (1999), p. 8.

79 European Parliament and Council Directive on a common framework for electronic signatures, <http://europa.eu.int/eur-lex/en/dat/2000/l_013/l_01320000119en00120020.pdf>. On this Directive see also: Kuner (1998), FIPR (1999) and Schulzki-Haddouti (1999).

harmonised legal framework for electronic signatures in the European Union. Currently, several EU Member States have issued or are planning to issue electronic authentication legislation, which may impede the development of electronic commerce due to their divergence.
The Directive starts off with a major and unfortunate limitation: it does not cover the legal recognition of electronic signatures related to the conclusion and validity of contracts or other non-contractual formalities requiring signatures (article 1). The Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market[80] does deal with the legal validity of electronic contracts (article 9), yet it does not affect signature requirements, since they are already covered by the Signature Directive. Thus, the EU Directive on electronic signatures will have confined significance.

The Commission supports a technology-neutral approach towards electronic authentication legislation, in an effort to ensure that the Directive will not become obsolete as technology and society progress. The explanatory memorandum of the draft directive formulated it as follows:

"While there is much discussion and work on digital signature technologies which employ public-key cryptography, a Directive at the European level should be technology-neutral and should not focus only on these kinds of signatures. Since a variety of authentication mechanisms is expected to develop, the scope of this Directive should be broad enough to cover a spectrum of "electronic signatures", which would include digital signatures based on public-key cryptography as well as other means of authenticating data".

The Directive does not limit the recognition of signatures to those created using a specific type of technology, indeed it uses the general expression electronic signatures , which is defined as:

"Data in electronic form attached to, or logically associated with, other electronic data and which serves as a method of authentication."

Similar to UNCITRAL Draft Uniform Rules, the Directive takes a hybrid approach in order to differentiate between different possible levels of reliability. The Directive therefore provides special legal consequences with respect to

[80] Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market, on-line available at: <http://europa.eu.int/comm/dg15/en/media/eleccomm/com586en.pdf>.

evidential issues to advanced electronic signatures. 'Advanced electronic signature' means:

"Electronic signature which meets the following requirements:
(a) it is uniquely linked to the signatory,
(b) it is capable of identifying the signatory,
(c) it is created using means that the signatory can maintain under his sole control, and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable."[81]

Sub (d) strongly relates to digital signatures and even though the EU Directive may leave room for future technologies to fulfil the rather high requirements of advanced electronic signatures, at present it seems particularly focussed upon the digital-signature technique.

3.2.2.3 Singapore

An example of the two-prong approach at a national level is the 1998 Singapore Electronic Transactions Act, which, *inter alia*, deals with liability of ISPs, electronic contracts, electronic records and electronic authentication.[82]
With respect to signing requirements,[83] the Act first generally states that an electronic signature may not be denied legal effect. Electronic signature means:

"Any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record."

Subsequently, special evidentiary presumptions are provided for secure electronic signatures, which are signatures made through an application of a

[81] Annex I determines that a qualified certificate contains the following: (a) the identifier of the certification service provider issuing it; (b) the unmistakable name of the holder or an unmistakable pseudonym which shall be identified as such; (c) a specific attribute of the holder such as, the address, the authority to act on behalf of a company the credit-worthiness, VAT or other tax registration numbers the existence of payment guarantees or specific permits or licences; (d) a signature verification device which corresponds to a signature creation device under the control of the holder; (e) beginning and end of the operational period of the certificate; (f) the unique identity code of the certificate; (g) the electronic signature of the certification service provider issuing it; (h) limitations on the scope of use of the certificate, if applicable; and (I) limitations on the certification service provider's liability and on the value of transactions for which the certificate is valid, if applicable."

[82] The Act is available from the Singapore Electronic Commerce Policy Page, <http://www.ec.gov.sg/policy.html>.

[83] Note that some provisions with legal requirements of form (e.g. will, negotiable documents, sale of immovable property) are excluded from this Act, see: Article 4.

prescribed security procedure or a commercially reasonable secure procedure. A security procedure being defined as

"a procedure for the purpose of (a) verifying that an electronic record is that of a specific person; or (b) detecting error or alteration in the communication content or storage of an electronic record since a specific point in time, which may require the use of algorithms or codes, identifying words or numbers, encryption, answerback or acknowledgement procedures, or similar security devices".

In addition, the Act requires a secure electronic signature to be:

"(a) unique to the person using it; (b) capable of identifying such a person; (c) created in a manner or using a means under the sole control of the person using it; and (d) is linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated".

Although at present these requirements will particularly be fulfilled by digital signatures, the Act leaves room for other (new) applications, which may fulfil these requirements as well by explicitly mentioning other techniques in its definition of security procedure and addressing (secure) digital signatures in Part VI of the Act. The digital signature is deemed a secure electronic signature if it is created in connection with a CA-procedure, which is in conformity with the rules set out in the Act.

3.2.2.4 Synthesis

Initiatives under the two-prong approach can be found at every level, the international, European and national level, and are generally of a recent date. In fact, there seems a tendency away from the digital signature approach towards a combination of digital and electronic signature legislation. All three (draft) regulations differentiate between electronic signatures and enhanced electronic signatures (though they use different terms for the latter), whereby enhanced electronic signatures especially (and at present exclusively) concern digital signatures. In this way, these initiatives aim at uniting the advantages of technology-neutral and technology-dependent legislation. Only the Singapore Act deals with requirements of form in an integral way by addressing both writings and signatures. The UNCITRAL Draft Uniform Rules merely deals with signatures, but there are cross-references (as far as signatures are concerned) to the UNCITRAL Model Law on Electronic Commerce dealing with formal requirements. However, the relationship between the Uniform Rules and the Model Law is not completely clear. Nor is it clear whether the Uniform Rules add something to the Model Law. From the Introduction to the Draft Uniform Rules, one can tell there has been a debate on the necessity of

the Rules, the widely prevailing view, however, was to continue work on these Rules.[84] Another restriction in both the Uniform Rules and the Model Law is their confinement to commercial contracts. The EU Directive addresses signature requirements but at the same time excludes the issue of the validity and conclusion of contracts from its scope. The latter subject is dealt with in the proposed E-commerce Directive and in its turn does not address signatures, because these will be regulated under the Electronic Signatures Directive. This twisted way of dealing with requirements of form may well be the result of difficulties the European Commission faced in trying to unite the divergent views of the EU Member States.[85]

The UNCITRAL Uniform Rules seem to take into account the functional approach (see section 2.3.3.) already adopted in the UNCITRAL Model Law, which leaves room for different legal systems to apply the rules.[86] The Singapore Act takes more of a Common Law approach towards electronic signatures, in that it does not so much address the purpose of signing as the fact that a signature shows the signer s expression of approval of the electronic declaration. In comparison with the other two examples, the EU Directive takes a rather restricted approach toward electronic signatures by merely providing certain reasons on the basis of which these signatures may *not* be denied legal effect.

The aforementioned shows that within the two-prong approach the regulations may still be very different, due to policy and other considerations as well as the legal system these initiatives originate from. These differences, unfortunately, do not contribute to transparency in the field of electronic authentication legislation.

3.2.3 The minimalist approach

The minimalist approach is a minimal way of regulating electronic authentication methods. This kind of legislation does not address specific techniques and, therefore, intends to be technology-neutral. In this approach, legislation relates to the functions, which signatures may have to fulfil in trade, and the different levels of reliability with respect to the purposes signatures are used for. Because this approach s main focus is on the relevant functions of signatures and the ways in which these functions may be translated into technological applications, it is also called the functionalist approach. Within the minimalist approach, the focus on functions of signatures (and writings) can be more or less explicit. Both the UNCITRAL Model on Electronic Commerce

84 Draft Uniform Rules on electronic signatures, A/CN.9/WG.IV/WP.82, 29 June 1999, no. 7 and 8.

85 See Kuner & Miedbrodt (1999), p. 149 and Schulzki-Haddouti (1999).

86 See, for instance, articles 3 and 6 of the Draft Uniform Rules.

(see paragraph 3.3.1.1) and the draft Electronic Commerce Framework Bill (see paragraph 3.3.1.2) of the Victorian government generally leave room to take into account these different functions. None the less, they do not give full review of legal requirements of form to identify functions and translate these into the electronic environment. In this respect, the approach taken in the Model Law and the draft Bill differs from the approach proposed by Huydecoper/Van Esch, which would call for systematic analysis of existing legal requirements of form and the considerations behind them.

3.2.3.1 UNCITRAL

One of the first regulatory initiatives with respect to electronic authentication, which embraces the minimalist approach, is the UNCITRAL Model Law on Electronic Commerce.[87] The UNCITRAL has adopted this Model Law under its mandate to promote the progressive harmonisation and unification of international trade law. The Model Law offers national legislators a set of internationally recognised rules as to how a number of legal obstacles may be removed and a more secure legal environment for electronic commerce could be achieved.[88] The Model Law is not a binding law, but an example for national legislators of how to deal with, *inter alia*, legal requirements of form in an electronic environment.

The Model Law, as a framework law, does not set forth all the rules and regulations that may be necessary to implement those techniques in particular country.[89] Countries that want to implement an act on this subject should supplement the Model Law with technical regulations to fill in this framework observing the Model Law s objectives. Although the Model law does not explicitly refer to industry self-regulation and co-regulation, one might assume that technical regulations can also be implemented using these regulatory instruments.

The terminology, which is used in the Model Law, is open and broad. Thus, the UNCITRAL aims at providing a Model Law, which is acceptable for countries with different legal systems, by leaving room for variation, while ensuring that some barriers to electronic commerce can be effectively removed. At the same time, the UNCITRAL avoids putting forward certain technologies and provides a scheme, which starts from functions of signatures instead of from technological functionality.[90]

---

[87] On-line available at <http://www.uncitral.org>.

[88] UNCITRAL Model Law (1996), No. 2.

[89] UNCITRAL Model Law (1996), p.14.

[90] UNCITRAL Model Law (1996), No. 55: "[A]ny attempt to develop rules on standards and procedures to be used as substitutes for specific instances of "signatures" might create the risk of tying the legal framework provided by the Model Law to a given state of technical development."

The minimalist approach, which is called functional-equivalent approach by the Model Law, chosen by the UNCITRAL aims at adjusting national legislation to ICT developments while leaving legal requirements of form and legal concepts underlying those requirements intact. The functions and purposes of these requirements is the point of departure and the Model Law provides criteria for fulfilling these purposes and functions by means of technology.[91]

Article 7 of the Model Law deals with signatures. This article states:

"(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:
(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.
(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.
(3) The provisions of this article do not apply to the following: […][92]."

Paragraph 1 subsection (a) provides the basic legal functions of a signature, which in combination with subsection (b) may be extended to other functions necessary under certain legal provisions. The Guide of Enactment of the Model Law identifies several (legal, technical and commercial) factors, which may be taken into account to determine whether the method used was appropriate under paragraph 1:

"(1) the sophistication of the equipment used by each of the parties;
(2) the nature of their trade activity;
(3) the frequency at which commercial transactions take place between the parties;
(4) the kind and size of the transaction;
(5) the function of signature requirements in a given statutory and regulatory environment;
(6) the capability of communication systems;
(7) compliance with authentication procedures set forth by intermediaries;

[91] UNCITRAL Model Law (1996), No. 18: "The Model Law does not attempt to define a computer-based equivalent to any kind of paper document. Instead, it singles out basic functions of paper-based form requirements, with a view to providing criteria which, once they are met by data messages, enable such data messages to enjoy the same level of legal recognition as corresponding paper documents performing the same function."

[92] National legislators may fill in the exceptions.

(8) the range of authentication procedures made available by any intermediary;
(9) compliance with trade customs and practice;
(10) the existence of insurance coverage mechanisms against unauthorized messages;
(11) the importance and the value of the information contained in the data message;
(12) the availability of alternative methods of identification and the cost of implementation;
(13) the degree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the method was agreed upon and the time when the data message was communicated; and any other relevant factor."[93]

Paragraph 3 leaves room for exclusions, for instance, contracts for which governments would like to maintain the traditional requirements of form, such as paper documents and hand-written signatures.
Article 7 does not stand on its own and must be applied in combination with articles 6 (writing) and 8 (original), which also embrace the functional-equivalent approach:[94]

"When adopting the "functional-equivalent" approach, attention was given to the existing hierarchy of form requirements, which provides distinct levels of reliability, traceability and unalterability with respect to paper-based documents. For example, the requirement that data be presented in written form (which constitutes a "threshold requirement") is not to be confused with more stringent requirements such as "signed writing", "signed original" or "authenticated legal act."[95]

3.2.3.2 Victoria (Australia)

Another illustration of the minimalist approach is the draft Electronic Commerce Framework Bill of the State Government of Victoria.[96] In this Bill, Victoria embraces the minimalist approach of the UNCITRAL Model on Electronic Commerce.

The Bill defines electronic signature as:

"the result of a process applied by the person to a document in electronic form by which –

- the person authenticates the document and

[93] UNCITRAL Model Law (1996), No. 58.
[94] UNCITRAL Model Law (1996), No. 47.
[95] UNCITRAL Model Law (1996), No. 17.
[96] Electronic Commerce Framework Bill, Department of State Development, State Government of Victoria, Australia, December 1998, <http://www.vic.gov.au/stategov/ecfbp&b.pdf>.

- acknowledges that the document is being signed."

In section 5, the Bill states with respect to signatures:

"(1) A person may use an electronic signature for any purpose for which a signature is required or permitted by law.
(2) The effect of an electronic signature is the same for the purposes of any law as that of a manual signature.
(3)This section --
(a) applies despite any provision to the contrary made by the particular law;
(b) does not apply in relation to a particular transaction if the parties to that transaction otherwise agree or any of those parties reasonably requires a method of signing other than by electronic signature;
(c) does not apply to the extent to which its operation is excluded by section 8 in the case of a particular law."

The exclusions in section 8 concern, *inter alia*, testamentary instruments, trust, powers of attorney, court documents and documents concerning an interest in real property. The Governor in Council, moreover, has the authority to issue regulations, which prescribe additional exclusions or exempt laws from section 8. In addition, the Governor can issue regulations, which, if necessary, provide further elaboration on the part of the Bill concerned with legal requirements of form.[97]

The Victorian government is of the opinion that the private sector should lead and will, therefore, encourage the development of guidelines, codes and standards in the private sector. The Minister may approve initiatives of the private sector resulting in organisations and codes, which can provide guidance to participants in electronic commerce or facilitate electronic commerce, by notice published in the Government Gazette.[98]

3.2.3.3 Synthesis

The Victorian draft law is one of the most recent initiatives, which falls back on one of the first initiatives, namely the UNCITRAL Model Law, in the field of electronic authentication. This makes it seems as we are back to square one.
The approach taken in the UNCITRAL Model Law is truly international in attempting to leave room for different elaboration by national legislators. An example of which is the Victorian draft law. The starting point is the differences in legal systems and the wish to accommodate the legal systems. One

[97] Section 10.
[98] Section 9.

(international and national) step further would be to develop and implement international concepts of formal requirements.[99] In the short run this does not seem feasible: consensus is not likely to be reached easily and, if it is ever reached, (national) legislators must go through the difficult process of reconsidering and adapting existing concepts in their legislation.

The minimalist approach taken in the Victorian draft law is very minimal compared with the possibilities that the Model Law provides in article 7, because it generally equates electronic signatures with manual signatures. The draft law leaves room for further elaboration and exclusions from the main rule in order to enable variation. The minimal approach taken in the Victorian Bill may be due to the low(er) requirements, which signatures may have to meet in Common Law systems (see section 2.4).[100]

		Techn.-neutral	**Techn.-specific**	**Examples**	**Definition**
Digital signature approach	*Technical variant*	-	+	Germany	Setting digital signature as technical standard (no explicit legal consequences)
	Legal variant	-	+	Utah, Italy	Legal recognition of digital signature under certain conditions
	Organisational variant	-	+	Japan, Netherlands	Requirements for CAs
Two-prong approach		+	+/-	UNCITRAL (e-sig), EU, Singapore	Legal recognition of (secure) electronic signatures under certain conditions
Minimalist approach		+	_	UNCITRAL (e-commerce), Victoria (Australia)	Equation of electronic signatures with hand-written signatures

Table 3: Approaches in electronic authentication legislation

3.2.4 Evaluation of the approaches

Important assumptions on which we have based our conclusions in this paragraph are that the market is constantly on the move and we do not know what lies ahead as far as technological and e-commerce developments are concerned. Therefore, we feel it is unwise to issue detailed regulations and to determine specific business models, such as the PKI model, when it is by no

[99] See Kuner & Miedbrodt (1999), p. 151.

[100] Note that we have not made any inquiries into these requirements in the Australian legal system; our remark is a mere presumption based on what we wrote in section 2.4.

means clear, whether they turn out to be viable models.[101] Viewed in this light, the digital signature approach is seriously flawed. Although, the legislators and regulators under the digital signature approach may have done so for all the right reasons (legal certainty, trustworthiness with respect to legal matters), the approach as such is not recommendable. The argument that digital signature legislation can offer more legal certainty and security because of its detailed character is untenable if such legislation proves to be obsolete or adjustable at any given moment:

"There is a growing assumption that existing electronic signature laws will need to be revised as the use of certification and electronic signatures expands and electronic commerce evolves, supplemented in some areas and streamlined in others. In addition, significant redrafting may be necessary if uniform laws are to be promulgated among different jurisdictions."[102]

The same is true, but to a lesser extent for the two-prong approach. The two-prong approach attempts to skirt around these problems by presenting an opening for new technologies besides setting criteria for certain advanced electronic signatures, which at present most notably cover digital signatures. The approach is understandable in the sense that there seems to be a strong inclination to look for clear and trustworthy solutions, while at the same time, there is a need to leave room for new solutions. Still, within the two-prong approach legislation often deals with issues and situations (e.g., CAs, liability, qualities that focus mainly on certain techniques), which have not yet been determined and thus, may well need adjustment once they have. In view of this situation, it is in our view not sensible at present to ask governments to implement PKI or similar models according to detailed rulings. Finally, both the digital signature approach and the two-prong approach are in many instances focussed too narrowly on signatures as such and not on formal requirements as a whole.[103]

---

101 Moreover, alternative models for traditional PKI are being developed already. See Brands (1999), who has developed alternative techniques, which unlike traditional PKI would provide privacy protection. Other models have also been developed, for instance, the SDSI (Simple Distributed Security Infrastructure) model of the Cryptography and Information Security Group Research Project, <http://theory.lcs.mit.edu/~cis/sdsi.htmlSDSI#>.

102 Australia (1998), paragraph 3.3.6. See also FIPR (1999), indicating situations and technologies, which are presently not covered by the EU Directive on Electronic Signatures.

103 See further paragraph 4.2.

As far as we are concerned, we are back to our starting point with the minimalist approach taken in the UNCITRAL Model Law still offering the most sensible solution to legislators wanting to tackle the problem of formal requirements in their legislation. Under this approach, legal requirements of form are generally dealt with in their entirety. Moreover, the minimalist approach allows for different functions which techniques have to fulfil under national legal systems, while creating room for new techniques and adventitious developments. Recent legislative initiatives recognise the advantages of the minimalist approach and have explicitly taken the UNCITRAL Model Law on Electronic Commerce as an example.[104] Whereas elaboration of legislation along the lines of the minimalist approach will most likely be of a national character, taking national considerations into account, it also has the potential to provide an international direction for a redefinition of the signature concept and for future uniform legislation.[105]

More detailed, technologically oriented legislation may still be an option when markets and technology are more clearly shaped and there is still a need to explicitly promote certain solutions. By then, the real problems may be clear enough to address them with more specific rules. Currently, the one problem is legal uncertainty and where that problem can be settled with a more general approach that solution is preferable. In the meantime, governments can take a co-operative stance toward international organisations and industry (and vice versa) and address subject matters, which are more clearly outlined already. Co-operation would provide as an additional advantage education of government officials with respect to developments in the market, since that aspect often leaves much to be desired.[106] Considering the need for a flexible and preferably international approach, co-regulation could be considered as an instrument to effectuate and reflect the co-operation between governments, international organisations and industry. The minimalist approach is likely to leave room for self-regulatory initiatives.[107]

---

104 Such as the Victorian draft law (paragraph. 3.3.1.2) and the Canadian the Uniform Electronic Commerce Act (UECA) (paragraph 4.4.2.2).

105 See for a first international attempt the Draft International Convention on Electronic Transactions, which the U.S.A. proposed to the UNCITRAL. Available at: <http://www.uncitral.org/english/sessions/wg_ec/wp-77.htm>.

106 See also Kuner/Miedbrodt (1999), p. 151.

107 See UNCITRAL Model Law (1996), Nos. 13-14.

4. Minimalism: exploring the functionalist approach

4.1 Introduction

In the previous paragraph we have classified and analysed the approaches toward electronic authentication regulation. These approaches include the digital signature approach, the two-prong approach and the minimalist approach. For reasons stated in paragraph 3.2.4, we prefer the minimalist approach as the way of addressing legal requirements of form in legislation. The minimalist approach does not address technology or certain models, but takes the functions of form requirements as the starting point and thus is of a functionalistic character. In this chapter we will further explore the minimalist approach by concentrating on this particular nature, which we will call functionalism.

4.2 Functionalism in general

The central question in the functionalist approach towards legal requirements of form is whether electronic signatures can fulfil the same functions as traditional signatures and, thus, replace these signatures in an electronic environment. The question could even be broadened by looking for a redefinition of the hand-written signature for electronic environments in order to meet with legal requirements of form and their functions. In other words, in what ways can the hand-written signature be replaced by digital techniques and still perform the same functions the legislator had in mind when including formal requirements in the law. The hidden presumption behind the broader question is that other techniques, which are not considered electronic signatures, may either in combination with or without electronic signature techniques fulfil functions behind signature requirements. For instance, some legal requirements intend to provide consumer protection by requiring a signed writing. In an electronic

environment there may be other means, not perceived as electronic signatures, which can fulfil that function as well as for example the general conditions appearing in pop-up screens, which need to be explicitly accepted by the consumer before he can proceed in the ordering process.
Further scrutiny of the functionalist approach shows that this approach falls into two separate working methods. First, the functionalist approach can be carried out by systematically reviewing legal requirements of form in legislation. This method involves reassessing every single formal requirement and the legislator's considerations as to why the specific formal requirement had to be included in legislation. On the basis of the outcome of that examination, the status of electronic authentication methods as a replacement for traditional signatures must be determined: can the electronic signatures fulfil the functions of hand-written signatures for the purpose of compliance with this specific legal requirement of form? An example of this approach is the functional-analysis test elaborated by Huydecoper/Van Esch.[108] Henceforth, called the specific-functionalist approach.
The second working method also takes into account the functions of traditional signatures and the fulfilment of these functions by electronic authentication methods, but does not require a systematic review of national legislation.[109] The use of electronic means for complying with formal requirements is allowed under certain conditions and, if necessary, with certain exceptions. This method is followed by the UNCITRAL in the Model Law on Electronic Commerce and the Victorian government (Australia) in its draft Electronic Commerce Framework Bill (see paragraph 3.2.3). We will call this approach the generic-functionalist approach.

4.3 The specific-functionalist approach

4.3.1 The working of the specific-functionalist approach

4.3.1.1 General

A test for the specific-functionalist approach has been worked out in the earlier mentioned study by Huydecoper/Van Esch: *Writings and Signatures: An Outdated*

[108] Huydecoper/Van Esch (1997).
[109] Although this approach could be combined with a long-term policy of reviewing the formal requirements as well.

Concept?.[110] This study identified, *inter alia*, functions of signatures in Dutch legislation and developed the functional-analysis test to determine whether electronic signatures and electronic documents can comply with formal requirements in the same way as hand-written signatures and paper documents can.

Huydecoper & Van Esch identified the following functions of signatures with respect to Dutch law:

- *Identification*. The addressee can verify the signer's identity by checking the signature.
- *Authentication*. The signature authenticates the declaration, which is included in the writing concerned. The writing reflects the facts correctly, unless evidence to the contrary is produced.
- *Declaration of will*. By signing the signer manifests his will and declares to be legally bound to the intention included in the writing concerned.
- *Authorisation*. The signer implicitly declares being authorised to perform a legal act, e.g., in case of representation.
- *Safeguard against undue haste*. By putting one's signature to a document the signer is notified that legal consequences may be involved. Thus, the signer is protected against undue haste.
- *Non-repudiation of origin and/or receipt*. The signer cannot deny that he has sent or received a document, unless proven otherwise.
- *Notice of contents*. The signer implicitly indicates that he knows the contents of the document.
- *Integrity*. Putting one's signature at the end of the document guarantees to some extent that the document has not been altered afterwards, thus, reducing the possibility of fraudulent actions.
- *Originality*. Signing a document enables to distinguish the original from a copy.[111]

As mentioned earlier, the functions of signatures have to be regarded in connection with those attributed to writings. Thus, it is significant to keep these

---

110 Huydecoper/Van Esch (1997). The title of this earlier study is, however, somewhat misleading, since it does not address the question of whether writings and signatures are indeed out-of-date concepts. The question is interesting though in the sense that in the electronic context there may be far more different ways of performing the functions of writings and signatures. Also in some instances electronic communication may not require these functions in the same way the paper environment does. See, e.g., Kuner/Miedbrodt (1999), p. 13.

111 Huydecoper/Van Esch (1997), p. 119-23. See also UNCITRAL Model Law (1996), No. 53.

functions in mind as well, when actually evaluating formal requirements in the light of electronic transactions.

4.3.1.2 Features

In their study, Huydecoper & Van Esch proceed to evaluate each function in the light of electronic signature techniques after having compared the features of hand-written signatures and electronic signatures first.[112] The reason why the hand-written signature was considered to be an appropriate means to fulfil the aforementioned functions is due to certain features of these signatures. Hand-written signatures are:

(1) Easy to use
(2) Durable
(3) Directly discernible
(4) Individual[113]

Electronic signatures and other techniques, however, do not in every instance display similar qualities.

(1) For users it is not always transparent what actually happens when applying electronic signature techniques, for instance, entering a PIN-code or using digital signature software, such as Pretty Good Privacy. Even though the global functioning of a technique may be clear to some users, the elaborated process may still be far too complicated to be fully grasped by most users. Electronic signature techniques are certainly far more complicated than hand-written signatures and (as yet) not always user-friendly. Apart from a lack of transparency and the complexity of the process, the electronic signer needs hardware and software to sign instead of merely pen and paper.
(2) Durability is problematic in an electronic environment. Electronic documents and signatures are nothing more than a set of bits & bytes, stored in the volatile memory of a computer, on the hard disc of a PC or server, or any other (portable) disc. Durability of electronic signatures is, thus, strongly dependent on the durability of the medium they are stored on, the carefulness of the user and/or owner of that medium and the durability of the software that is used.
(3) Electronic signatures are not directly discernible. The user needs access to hardware and the appropriate software in order to check the signature. However, the control process in which the validity of the signature is

[112] Huydecoper/Van Esch (1997), p. 118-9.
[113] Huydecoper/Van Esch (1997), p. See also UNCITRAL Model Law (1996), No. 48, with respect to writings.

checked may, in many instances, probably be quicker and more reliable where electronic signatures are concerned.

(4) Electronic signatures are in principle not individual, meaning that they are not inherently linked to a certain person, as is the case of hand-written signatures. This may be different as far as certain electronic signatures are concerned, that use personal features of the signer, also called biometric features, such as fingerprints, iris, pressure and speed of signing (digital pen), and the appearance of the signature (scanned signature). Biometric techniques do, however, show drawbacks, which are mentioned in the following section (paragraph 4.3.1.3).[114]

4.3.1.3 Functions

In pursuance of this comparison of features, the evaluation of functions with respect to electronic signature methods, in our opinion, shows the following picture.

With respect to *all* the functions, the non-individual character of electronic signature techniques seems to be the major obstacle. For instance, electronic signatures are not appropriate means of identification and authentication by themselves, since they lack individuality: they are not inherently connected with one individual.[115] Thus, electronic signatures need to be used in combination with other technical and security measures to be able to fulfil the identification function. Many electronic signature regulations, therefore, provide a system of digital certificates,[116] which may have shortcomings with respect to, e.g. privacy implications.[117]

In Huydecoper & Van Esch's opinion, biometric identification methods "indisputably determine the user's identity". However, this is stated far too easily, since biometrics is certainly not a one hundred percent reliable means of identification. This is due to the fact that these methods are based upon probabilities, meaning that a certain failure rate exists. Moreover, some biometric features are less stable (e.g. dynamic signatures) than others (e.g. iris and finger print) and the unique status of several biometric features is still disputed. Thus many biometrics applications may seem too unreliable to serve

---

114 Huydecoper/Van Esch (1997), p. 132-4.

115 As a result of privacy dangers in electronic communication, the role of identification may possibly have to change with respect to electronic transactions. In our view, heavy requirements for identification would be unjustified where verification of, e.g., authority is sufficient.

116 For instance, on the basis of a PKI-system, but there are other alternatives as well, e.g., SDSI. See on SDSI: <http://theory.lcs.mit.edu/~cis/sdsi.html>. See also Brands (1999).

117 See Brands (1999), who developed techniques that meet privacy requirements.

as an authentication means.[118] Furthermore, there is the problem of maintaining a directory, in which biometrics are linked to persons. Otherwise there is no way of knowing whether a biometric feature, e.g. an iris print, attached to a an electronic message, belongs to a certain person.[119] Finally, there might even be objections to biometrics of a more ethical nature, because some of the techniques may not (yet) be completely accepted by users.[120]

As regards the integrity function of signatures, electronic signature techniques will in principle not be the most suitable means in an electronic environment to perform this function. Electronic signatures, as electronic documents, are merely a collection of bits & bytes, which may in general be easily manipulated. An exception is the digital signature, which on the contrary is excellently apt to guarantee the integrity of electronic documents.

An electronic original, strictly speaking, does not exist. Additional technical measures will always be necessary to determine and secure certain versions of electronic documents. Again digital signature applications may possibly be an adequate means to approximate the originality concept especially in combination with time-stamping techniques.

As a result of the lack of experience with electronic-signature techniques, the undue-haste and notice-of-contents functions seem not to be fulfilled properly by using these techniques. By putting a hand-written signature to a document, sometimes in combination with other ceremonial aspects, for instance, appearing before a notary public, the signer will most likely be aware that a matter of legal importance is about to occur. Electronic-signature techniques, however, do not have (as yet) the same connotation and it is by no means certain that these techniques will ever have a similar impact, since they do not exactly shine in user-friendliness and the underlying technical processes are usually not very transparent to the common user.[121]

To conclude this paragraph, it is clear that electronic-authentication techniques do not necessarily provide alternatives to hand-written signatures in themselves. Often additional measures are necessary to adequately fulfil most of the functions.

---

118 Kralingen, Prins & Grijpink (1997), p. 21. Ongoing research on biometrics will, however, result in further improvement of these techniques.

119 Personal communication by John D. Gregory.

120 Kralingen, Prins & Grijpink (1997), p. 54-55.

121 There are, however, developments to integrate authentication techniques in software in order to contribute to the user-friendliness of these techniques.

4.3.2 Proposals for the specific-functionalist approach

4.3.2.1 The Netherlands: Huls-report

In 1998, the Dutch Cabinet instructed the Huls-commission[122] to examine the necessity of existing formal requirements and equivalent electronic alternatives for formal requirements where these requirements are still necessary as well as conditions for the use of electronic alternatives. [123] The commission carried out its investigations on the basis of three examples of formal requirements in Dutch law:

(1) Employment contracts;
(2) Transfer of immovable properties;
(3) Announcement obligation for administrative decisions.[124]

The Huls-commission opts for a specific-functionalist approach towards formal requirements. This approach would consist of a functional analysis, because each formal requirement needs to be checked against the legislator s considerations for implementing the particular formal requirement. The Huls-commission report elaborates every example on the legislator's reasons for implementing the formal requirement in the law and subsequently the conditions for performing these formal requirements electronically. With respect to each of the aforementioned examples, the commission concludes that electronic performance of the formal requirements is possible under certain conditions. These conditions (unsurprisingly) focus on the specific functions that the formal requirements have to fulfil.
The Huls-commission indicates three functional distinctions, which the legislator should take into account when addressing laws for electronic environments. First, the evidence and communication functions of (electronic) documents are important for social acceptance of new techniques. Second, there is a difference between open and closed networks. Closed networks are confined to a limited number of parties with a certain (contractual) relationship. Open networks are publicly accessible. Acceptance of electronic documents is sooner expected in a closed environment than in an open one. Thirdly, consumers and professionals need to be distinguished. It is important to ensure

122 This commission was named after its chairman Professor Huls.

123 Startnotitie Elektronisch verrichten van rechtshandelingen, Huls-report (1998), Annex I.

124 These examples have been criticised, because they were found not to be relevant to electronic commerce, see Van Esch (1998), p. 303. However, there are already examples of on-line legal forms in the field of, e.g., family law, sales, real estate and employment, see Matthijssen (1997), p.19-21.

consumer protection by, for instance, introducing time for reflection as is provided by the European Union Directive on Distance Selling.[125]
This being considered, the commission addresses the virtues of self-regulation, especially in situations where technology is developing and self-organisational market forces are at work. The government will often not be able to influence these developments, but may still set conditions to structure self-regulatory initiatives in the market (conditioned self-regulation). However relevant self-regulation may be, it is, according to the commission, still important that the government issues legislation. Therefore, the Huls-commission proposes to the legislator to implement so-called experimental provisions (or in other words: trial-and-error provisions) into Dutch law, which allow electronic communication where formal requirements exist and set conditions accordingly. Test-provisions, being an unknown phenomenon in Dutch law, seem to be the result of the commission understanding that something needs to be done with respect to requirements of form, but they feel hesitant about actually doing anything about it. Communication with the Ministry of Justice revealed that meanwhile test-provisions will not be used, due to the wave of criticism about this indefinite concept.
The trial-and-error legislation issue was most certainly raised as a means to provide conditions in abstract wordings, which would leave room for self-regulation and case law to fill in the gaps. These abstract conditions would include principles with respect to integrity, transparency, voluntariness, confidentiality, availability, protection from undue haste, durability and authenticity. The commission does, however, not indicate more concretely what these experimental provisions would actually have to be like.

On the one hand, the Huls-commission seems to adhere to the functional-analysis approach by stating that each formal requirement must expressly be analysed concerning their ability to be complied with electronically. On the other hand, the Huls-commission takes a more open approach by putting forward general principles for formal requirements, while leaving further elaboration to self-regulation and case law. As we understand it, the functional analysis of formal requirements needs to be performed by the users of electronic-communication means as well as by judges, according to the general principles the commission put forward. In our opinion, this is an impassable road for several reasons. First of all, the functional analysis of formal requirements is, as we know from experience,[126] a time-consuming and

[125] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the Protection of Consumers in respect of Distance Contracts, <http://europa.eu.int/comm/dg24/policy/developments/dist_sell/dist01_en.html>.

[126] Our initial plan was to include examples (such as article 2 Dutch Copyright Act 1912) of such analyses in this report, but in performing the functional analysis test we realised that it is

cumbersome process and certainly not something that should have to be performed on the user level for each formal requirement individually. In addition, the principles set by the commission would provide too little guidance in that respect. Therefore, this approach will not provide the necessary legal certainty. The same is true for case law. Although, judges are better equipped for functionally analysing formal requirements, it is unfeasible having to sit and wait for probably a long time for answers that are needed today. Finally, the solution presented by the Huls-commission unfortunately does not urge the legislator to rethink formal requirements as such and examine whether they are still up to date. [127]

4.3.3 The Draft EU Directive on Electronic Commerce

The EU Draft Directive on Electronic Commerce addresses formal requirements in article 9, by stating that Member States have to:

"Ensure that the legal requirements applicable to the contractual process neither prevent the effective use of electronic contracts nor result in such contracts being deprived of legal effect and validity on account of their having been made electronically."

Notice that signatures are not included here, because the EU Directive on Electronic Signatures is said to be dealing with the subject. This is, however, not completely true, since in its article 1 the E-signatures Directive excludes aspects related to the conclusion and validity of contracts or other legal obligations.
Article 9 does not mention the way in which Member States should be dealing with formal requirements in their legislation. In the Explanatory Memorandum of the Directive, however, a strong indication exists that Member States will have to take the functional-analysis approach in that a systematic review of legislation is required:

"The Member States have an *obligation to succeed*, carry out *a systematic review* of those rules which might prevent, limit or deter the use of electronic contracts and to carry out *this review in a qualitative way*, i.e., not seek simply to amend the key words in the rules (e.g. "paper") but to identify everything which might in practice prevent the

---

sheer drudgery and, thus, certainly not the proper way to a reasonably speedy solution of legal uncertainty with respect to formal requirements.

127 Kuner & Miedbrodt (1999), p.13, It is crucial that there is a realistic assessment by policymakers of the extent to which formal requirements that have traditionally been recognised in national legal systems remain relevant in the digital context. For instance, the warning function of written form may be less important in an electronic environment.

"effective" use of electronic contracts." (Italic by the drafters of the draft directive)[128]

Since, however, the method of adjusting formal requirements to enable electronic contracting to the fullest potential is not named explicitly, other methods of working may be permitted as well. As long as the Member States live up to the obligation to succeed in allowing electronic contracting notwithstanding the existence of formal requirements.

4.4 The generic-functionalist approach

4.4.1 General

The second method under the functionalist approach, what we call the generic-functionalist approach, does not require a thorough review of form requirements in legislation, neither does it provide detailed rulings for electronic communication. The generic-functionalist approach is based on basic principles, which are derived from the functions of form requirements. These principles do not have to represent every imaginable feature and function of signatures, writings and other form requirements, but should at least hold basic conceptions of relevant criteria for electronic communication. Where the application of these principles is less obviousness, there is the possibility to make an exception with respect to certain form requirements.[129]

4.4.2 Illustrations of the generic-functionalist approach

4.4.2.1 UNCITRAL Model Law on Electronic Commerce

The generic-functionalist approach is embodied in the UNCITRAL Model Law on Electronic Commerce, where it is called the functional-equivalent approach.[130] Most notably, the articles 6 to 8 are relevant to form requirements.[131] In these provisions, the UNCITRAL has set up a hierarchy of

128 Proposal EU-Directive E-commerce (1998), p. 25, <http://europa.eu.int/comm/dg15/en/media/eleccomm/com586en.pdf>.

129 See, for instance, the exceptions in Section 8 of the Victorian draft law (paragraph 3.2.3.2).

130 See UNCITRAL Model Law (1996), No. 16. Because the term 'functional-equivalent approach' could easily be confused with the specific-functionalist approach, we will further use the term 'generic-functionalist approach'.

131 UNCITRAL Model Law (1996), No. 47, these articles should be read in coherence with each other.

form requirements, requiring different levels of reliability, traceability and inalterability. This hierarchy goes from writings, signed writings up to signed originals.[132] Thus, the UNCITRAL has not looked for one-to-one equivalents but:

"single[d] out basic functions of paper-based form requirements, with a view to providing criteria, which, once they are met by data messages, enable such data messages to enjoy the same level of legal recognition as corresponding paper documents performing the same function."[133]

Schematically reproduced, the provisions 6 to 8 provide the following, reversibly represented hierarchy:

Form requirement	**Criteria**	
Writing	Information is accessible: usable for subsequent reference	
Signed writing	Identification of a person	
	Indication of person's approval of the information	
	Reliability (depending on the purpose of data message)	
Signed original	Reliable assurance of integrity	Completeness
		Inalterability
		Depending on purpose of information generation
	Display of the information	

Table 4: Hierarchy of form requirements

The provisions leave room for exceptions, however, the intention is not to enable blanket or numerous exceptions, which would bring down efficacy of the Model Law.[134]

4.4.2.2 Other examples: UETA, UCITA, UECA

In paragraph 3.2.3, we have already mentioned the Victorian draft law as an illustration of legislation using the UNCITRAL Model Law as an example. The generic-functionalist approach introduced by the Model Law has also been followed in other (draft) legislation, such as the Draft Uniform Electronic Transactions Act (UETA)[135] and the Draft Uniform Computer Information Transactions Act[136] in the United States[137] and the Uniform Electronic

132 UNCITRAL Model Law (1996), No. 17, 49.
133 UNCITRAL Model Law (1996), No. 18.
134 UNCITRAL Model Law (1996), No. 52. The possibility to make exceptions should add to the acceptability of the Model Law.
135 Available at <http://www.law.upenn.edu/library/ulc/ulc.htm#ueccta>.
136 Available at <http://www.law.upenn.edu/library/ulc/ulc.htm#ucita>.

Commerce Act (UECA) of Canada.[138] Although these laws probably drew inspiration from the Model Law,[139] the end result is, however, tailored to national situations. All three examples mentioned - UETA, UCITA, and UECA - put great emphasis on the principles of freedom of contract and technology neutrality. These laws provide a framework or minimum requirements for electronic transactions, but parties are free to agree on other or heavier requirements: in the same way parties concluding a contract orally often want to confirm the contract in paper.[140] Neither of these laws prescribes certain techniques to fulfil formal requirements and all of them have open definitions of 'electronic', 'electronic documents' (messages or records) and 'electronic signatures' (authentication).[141]
Both UETA and UECA follow the hierarchical pattern of the UNCITRAL Model Law by addressing writing, signed writing and signed original.[142] UCITA more generally addresses electronic records and authentication, stating that these methods may not be denied legal effect, leaving it to the parties concerned to set their own requirements[143] and sets specific requirements for proof of authentication.[144]

All three initiatives - UETA, UCITA and UECA - are drafted, however, within a Common Law system. The Civil Law elaboration of the principle of minimalism may well be shaped differently. Most likely, Civil Law systems would put an emphasis on the implementation of reliability requirements with respect to electronic documents and electronic signatures.[145] At present, there are no readily available (draft) laws in Civil Law countries that start from the minimalist or more specifically the generic-functionalist approach.[146] The Dutch Ministry of Justice is, however, examining the application of the generic-functionalist

137 Both the UETA and the UCITA are drafted by the National Conference of Commissioners on Uniform State Laws.

138 Available at <http://www.law.ualberta.ca/alri/ulc/current/euecafa.htm>.

139 The UECA is explicitly based on the UNCITRAL Model Law, see introductory remarks in the UECA.

140 See Section 107 of UCITA and Section 5 of UETA. See also introductory remarks in the UECA.

141 See Section 102 UCITA, Section 2 UETA and Section 1 UECA.

142 See UETA Sections 7-11 and UECA Sections 7 (Requirement for information to be in writing), 8 (Providing information in writing), 9 (Providing information in specific form), 10 (Signatures) and 11 (provision of originals).

143 See Section 107 and the explanatory comments on that section.

144 See Section 108.

145 See paragraph 2.4.

146 A few years ago, the Danish government announced their intention to draft legislation based on the UNCITRAL Model Law on Electronic Commerce, but the draft law that was finally presented is concerned with digital signatures and Certification Authorities. Available at: <http://www.fsk.dk/fsk/div/hearing/draft.html>.

approach in administrative law (electronic administrative decisions) and there may be other initiatives in Civil Law countries that have not yet surfaced.

4.5 Evaluation of the specific-functionalist and generic-functionalist approach

Having described both the specific-functionalist and generic-functionalist approach, it is time for an evaluation of these approaches before drawing conclusions.
A strong argument in favour of the functionalist approach generally is the open attitude towards new techniques as well as future developments it allows rather than discouraging electronic commerce activities with premature and inflexible legislation. Furthermore, the functionalist approach seems to be better suited to deal with formal requirements in its entirety. In the case where situations have crystallised out and prove to need further regulation after all, more detailed rules can still be issued (for instance in the form of co-regulation). Having made these general remarks, we will now more particularly address the specific-functionalist and the generic-functionalist approach.

The **specific-functionalist approach** does justice to the diversity in formal requirements and, thus, the different reasons for having these requirements in laws. Every formal requirement can be judged on its merits and accordingly adjusted to electronic communication. Moreover, the legislator can more fundamentally examine the necessity of formal requirements in general or with respect to electronic communication in particular and abolish outdated requirements completely.
The functional-analysis test is, however, most notably suitable for legislators when actually wanting to update existing formal requirements as a long-term project. Reviewing each and every formal requirement is a very cumbersome and time-consuming process. Dutch law alone contains many formal requirements,[147] which have been included in the law for different reasons and not in every instance these reasons are obvious from the law itself or its Explanatory Memorandum. In addition, reviewing the law in such a detailed way brings an extra danger of looking for detailed solutions as well. In other words, in our experience it is difficult to avoid technology-dependent ways of dealing with formal requirements under the functional-analysis approach, as a result of which the law may become too rigid and closed to new developments. There is now a situation where we do not and cannot know all the possible techniques

147 See a non-exhaustive list of formal requirements in Huydecoper/Van Esch (1997), p. 77, Note 16 and p. 177.

and their legal implications, which is different from the once surveyable paper environment where only paper and pen existed. But the inclination to look for equivalent techniques in order to make the subject matter manageable would be all too human.

The **generic-functionalist approach** is no match for the thoroughness of its specific counterpart. In the specific-functionalist approach requirements of form are more fundamentally being dealt with, because of its systematic review of each and every (or the most relevant) requirements. In the process, outdated formal requirements can de identified and removed from legislation. The generic-functionalist approach is a rougher way of dealing with the issue in that it will generally be blind to the nuances of form requirements.
On the other hand, the generic-functionalist approach displays greater flexibility in having the ability to provide a swifter solution to the problem of form requirements. This approach does not necessarily require a systematic review of each form requirement. It would suffice to distil objective criteria by generally analysing the functions of forms that are found relevant in judicial matters and more specifically electronic communications. The UNCITRAL Model on Electronic Commerce presents an excellent example of how to perform such an analysis. In case of doubt, the legislator can exclude certain form requirements from the general ruling and decide to subject these requirements to further scrutiny. The specific-functionalist approach and the generic-functionalist approach are not mutually exclusive and, if necessary, the former can be supplemental in special instances. This may alleviate some of the roughness of the generic-functionalist approach.
Moreover, the generic-functionalist approach per definition has a technology-neutral character, because the legislator will be forced to look for general rather than detailed rules. In addition, the generic-functionalist approach leaves room for possible, future international approaches to form requirements in electronic commerce. The specific-functionalist approach is too focused on the national position to also allow for an international method of approach.[148]

4.6 Conclusion

In this chapter, we have analysed and evaluated two approaches under the functionalist approach: the specific-functionalist approach and the generic-functionalist approach.

[148]See Kuner & Miedbrodt (1999), p. 150, "The international legal acceptance of electronic authentication technologies will be impeded if each legal system clings to its own parochial conception of what constitutes a signature, which will also lead to increasing trade disputes and international tension."

The specific-functionalist approach is concerned with identifying functional equivalents to writings and signatures for fulfilling specific form requirements electronically. The central question under this approach is: can electronic techniques fulfil the same functions as writings and signatures, considering all the reasons for legislators to include this form requirement in legislation in the first place and under what conditions? An affirmative answer to this question would mean that (certain) electronic documents and signatures are adequate for complying with the formal requirements at issue. Because this approach would signify a complete review of form requirements in national legislation, it does justice of the nuances of form requirements and provides a good opportunity to get rid of outdated form requirements. A drawback of this approach, however, is that it is cumbersome and time-consuming.
The generic-functionalist approach involves the formulation of general provisions, which indicate under what conditions electronic techniques can fulfil formal requirements. These conditions may include criteria with respect to the readability, reliability, inalterability, traceability etc. Depending on the basic functions of which it is paramount that they are fulfilled by writings, signed writings, signed originals etc., electronic communication may be legally recognised. This approach does not require a complete review of legislation, because basic principles will be applicable to electronic communication in general. In that respect, the approach has a rough edge which does not take into account the specifics of form requirements. The advantage of this approach, however, is that a more swift resolution of the form requirement problem is possible. Moreover, in the generic-functionalist approach the risk of focusing on specific technologies is minimal and there is room for possible, future international formula for the issue of form requirements.
It is, furthermore, important to notice that these approaches are not mutually exclusive: legislator's can decide to choose the one approach to solve things on a short notice and the other approach to more fundamentally address (some) form requirements as a long term project.

Having summarised the findings of this chapter, we now come to a conclusion. On the basis of the evaluation of the approaches and considering the need to make an end to legal uncertainty, we find a short-term solution and, therefore, the generic-functionalist approach, preferable to a solution that will take a lot of time to take effect, such as performing the functional-analysis test. Formal requirements are perceived a problem to electronic contracting today and the legislator should deal with issue on a short as possible notice. The legislator should, however, not completely sacrifice the virtues of the specific-functionalist approach and leave options for more fundamental assessment open in instances where the general principles prove to be too rough an instrument. Nevertheless, this should desirably be an exception to the rule.
Having dealt with the issue along the lines of the generic-functionalist approach, the legislators may still decide to perform a full review of form requirements. In

that process outdated form requirements can, for instance, be eliminated from legislation completely. Other interdependent issues for the long-term process, which the legislator should take into consideration, are the redefinition of certain concepts, e.g. the notion of traditional signatures, and international co-operation. Redefinition of form requirements may present an opening for addressing the legal aspects of electronic communication more uniformly on an international level.[149]

[149] See also Kuner & Miedbrodt (1999), p. 150-151.

5. Conclusions & recommendations

5.1 Introduction

To conclude this research report, all that remains is to formulate recommendations and to provide an integral presentation our observations and conclusions. The main aim of our research was to provide recommendations to the legislator when addressing legal requirements of form in legislation. In the following paragraphs we will address issues which the legislator should take into account in order to participate in clear discussions on electronic authentication and workable legislation concerning form requirements. These issues are:

(1) Terminological perspicuity
(2) Contextual perspicuity
(3) Minimalism

The order of these issues is not arbitrary, but reflects the chronology in which the legislator should deal with the subject of formal requirements in an electronic environment.

5.2 Terminological perspicuity

As obvious as it may seem, but before elaborating on a subject (in discussions, negotiations, legislation etc.) it is important to be clear as to the terminology used. As far as electronic authentication is concerned, it is unfortunately turning into a modern version of the Tower of Babel.
The term 'signature' may have different meanings for lawyers from distinct legal systems (most notably Common Law and Civil Law systems) and different

countries, as well as for lawyers and people with a technical background. Moreover, the terms 'electronic signature' and 'digital signature' are often used as synonyms, whereas from a technical viewpoint they can be clearly distinguished. Electronic signatures involve all technologies, which replace hand-written signatures in an electronic environment. Digital signatures are technological applications, which use asymmetric encryption to ensure the authenticity of electronic messages and the integrity of the contents of these messages.
Furthermore, 'electronic signature' and 'digital signature' are not uniform concepts: within these concepts different forms of techniques can be distinguished, which may be quite distinct with respect to their functions and their feasibility to "sign" electronic documents. Whereas the traditional forms (writing, paper, witnesses etc.) of performing legal acts were unambiguous, technology has many facets and is not as easily put into the straitjacket of formal requirements.
Before starting any legislative process, the legislator should have a clear picture of relevant and essential terminology with respect to the subject they intend to regulate. As the circumstances surrounding the realisation of the draft EU Directive on Electronic Signatures clearly show, confusion of tongues can be one of the reasons for a serious complication of the legislative process.[150]
In order to get a clear picture the legislator should seek the co-operation of academics and industry. Valuable information and advice can both nationally and internationally be obtained by involving different disciplines in the preparatory work and the process itself. Besides seeking advice, government officials should themselves be educated concerning the subject, since they have to be able to make choices in the matter.

5.3 Contextual perspicuity

Once having the terminology right, it is important to clearly see the different contexts of electronic authentication and formal requirements. Depending on the perspective one takes the consequences may differ.
One important difference in context is that of Civil Law systems versus Common Law systems. Electronic-authentication legislation is often mutually compared without expressly considering the fact that these systems differ a lot in the way formal requirements are being dealt with traditionally in each system. These traditional differences may, however, very well have an impact on how new legislation is or should be addressing electronic authentication or form requirements in electronic communication. Even within legal systems of the same family there may be dissimilarities, which could be a reason for regulating

[150] Dumortier & Van Eecke (1999b), p. 106-107.

these issues differently. Thus, when using (draft) legislation in other countries as an example, one should know about essential similarities and differences between the other and one's own legal system.
Moreover, it is important to keep an eye on the context as far as the international level is concerned. Having all these distinct systems on a national level, international approaches may adopt a middle course to satisfy the requirements of different legal systems. Whereas national legislation can be more concretely tailored to the national situation, international initiatives will probably adopt a more open or abstract language, in order to be acceptable to a large number of countries. Therefore, besides looking at differences between legal systems on a national level, one should also take into account these differences when evaluating initiatives internationally.

5.4 Minimalism

Once having attained terminological and contextual perspicuity, one can start to pursue the fundamental issue of how to actually address formal requirements.
In advance, it is significant to mention that form requirements should be dealt with coherently. Neither the situation where only signatures are addressed nor the situation where signatures are addressed in one legal instrument and other form requirements in another is preferable. Traditionally, signature, writing and other form requirements belong together, because a hand-written signature solely exists by the grace of paper, and should therefore be addressed together.
Since the market is constantly moving and we do not know what lies ahead of us as far as technological and e-commerce developments are concerned, the legislator should stay away from detailed, technology-dependent legislation. More detailed, technologically oriented legislation may be an option in the future, when markets and technology are more clearly shaped and there still turns out to be a need to expressly promote certain solutions in certain areas. By then, the real problems may be clear enough to address them by more specific rules.
For now, the legislator should rather take a minimalist approach towards form requirements and electronic communication. In the minimalist approach, legislation does not address specific techniques and models, such as digital signatures and PKIs. This approach allows for the different functions that techniques have to fulfil under national legal systems, in which case we have called it the functionalist approach, while creating openness towards new techniques and adventitious developments. These functions may be the ones that have to be fulfilled by traditional formal requirements, but it would also be possible to identify more general notions with respect to electronic communication, such as is the case with the UNCITRAL Model Law on

Electronic Commerce. The minimalist approach leaves room for self-regulation or co-regulation, if necessary.

Observing the principle of minimalism, the legislator can take two directions. Both present valuable ways of dealing with the subject matter.
The first one, the *specific-functionalist approach*, involves a systematic review of formal requirements. The analysis determines whether or not a form requirement can be complied with electronically or if it is outdated altogether. This analysis involves an examination of the considerations behind formal requirements and an assessment of whether electronic communication can satisfy these considerations. This solution allows a fundamental assessment of formal requirements. The drawback here is that reviewing each form requirement is a cumbersome and time-consuming process and is not likely to provide a solution soon.
The second way, the *generic-functionalist approach*, involves a more general solution. In this approach, the legislator drafts provisions containing general principles and criteria for electronic communication in general,[151] which remove uncertainty as to the legal status of electronic documents and electronic signatures. This approach allows a quicker resolution of the issue, but is blind to the nuances in considerations for the rationale of individual form requirements. At this point, we think the legislator should nonetheless primarily focus on the generic-functionalist approach to achieve a solution on short notice. We believe that the edges can be taken off this approach by allowing exceptions in hard cases, meaning that some form requirements can be excluded when the impact of a general provision needs more clarity in advance. Having dealt with the issue along the lines of the generic-functionalist approach, there is still room for performing a full review of form requirements, if found to be necessary. As a result of that review outdated form requirements can be eliminated from legislation completely.
Apart from a quicker resolution of the form-requirement problem, the generic-functionalist approach may in the course of time present an incentive for a more international approach to form requirements. An international approach is attractive because electronic commerce is an international phenomenon and it would remove some of the legal barriers caused by differences in legal systems. Before considering an international approach, it is however necessary to redefine form requirements and most notably the traditional signature for the international context, because of the different connotations the concepts have in the various legal systems. Part of the redefinition process could already take place when drafting generic rules for electronic communication.

151 The legislator may want to differentiate between different areas of law and provide separate principles for private law, criminal law and administrative law.

5.5 Final remarks

Here we have presented recommendations to legislators on which considerations should be taken into account when addressing the subject matter of legal requirements of form in the light of ICT developments. Before addressing the subject at all, terminological perspicuity and contextual perspicuity should be prerequisites. When addressing the issue itself, the legislator should observe the principle of minimalism and take a functionalist approach towards form requirements and electronic communication. The functionalist approach should be worked out by issuing general principles and criteria for electronic communication. In this study we have not elaborated on the actual contents of these general principles and criteria, apart from setting the UNCITRAL Model Law as an example. Aside from the fact that the definite development of these criteria will (still) depend on the legal system involved, we feel that further (international) research is necessary before it is be possible to further pronounce upon the subject matter.

This research was concluded on 1 December 1999. Later developments have not been included.

6. Literature

6.1 Books & articles

Arkenbout (1998) - E.J. Arkenbout, *Advice of the Copyright Commission*, Informatierecht/AMI 1998-9, p.161.

Baker & Yeo (1999) - S. Baker & M. Yeo, *ILPF Survey of Electronic and Digital Signature*, last updated: 24 September 1999. On-line available at: <http://www.ILPF.org/digsig/survey.htm>.

Baum (1999) - M. S. Baum, *Technology Neutrality and Secure Electronic Commerce: Rule Making in the Age of Equivalence* , Verisign Inc. 1999.
On line available at <http://www.com/repository/pubs/tech_neutral>.

Baum & Ford (1997) - M.S. Baum, W. Ford, Secure Electronic Commerce, Building the Infrastructure for Digital Signatures & Encryption, Prentice Hall New Jersey 1997.

Beary (1998) - E.B.J.D Beary, *The Digital Signature Debate: Technology Neutral or Specific?* , 1998. On line available at: <http://raven.cc.ukans.edu/~cybermom/CLJ/beary.html>.

Biddle (1997) - C. Bradford Biddle, *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace*, May 1997. On line available: <http://www.acusd.edu/~biddle/LMW.htm>.

Brands (1999) - S. Brands, Rethinking Public Key Infrastructure and Digital Certificates, 1999 (thesis). Part of it is on-line available at: <http://www.xs4all.nl/~brands/>.

Cerina (1998)- P. Cerina, *The New Italian Law on Digital Signatures*, CTLR 1998-6, p.193-199.

De Cock Buning (1998) - M. de Cock Buning, *De beperkte houdbaarheid van technologie-specifieke regelgeving* (The limited tenability of technology-specific legislation), Informatierecht / AMI 1998-8, p. 129-135.

Dumortier (1998) - J. Dumortier, *Multimediale wetgeving in Duitsland: een inspirerend voorbeeld*? (Multimedia legislation in German: an inspiring example?), CR 1998-1, p. 2-3.

Dumortier & van Eecke (1999a) J. Dumortier, P. van Eecke, *De Europese ontwerp-richtlijn over de digitale handtekening: waarom is het misgelopen?* (The European draft directive on the digital signature: why did it go wrong?), CR 1999/1, p. 3-10.

Dumortier & Van Eecke (1999b) - J. Dumortier, P. van Eecke, *The European Draft Directive on a Common Framwork for Electronic Signatures*, Computer Law & Security Report Vol. 15 No. 2 1999, p. 106-112.

Van Esch (1998) R.E. van Esch, *Werkgroep Electronisch verrichten van rechtshandelingen* (Working Group on electronic legal acts), CR 1998-6, p.302-305.

Van Esch (1999) - R.E. van Esch, Electronic Data Interchange en het Vermogensrecht (Electronic Data Interchange and the law of property), PhD thesis Nijmegen University, Deventer: Tjeenk Willink 1999.

Heineman (1999) - M.E. Heineman, *Over IP-adressen en de Wbp: grenzen aan privacybescherming op Internet* (About IP-addresses and the Act on the protection of personal data: limits to privacy protection on the Internet), Privacy & Informatie 1999/4, p. 148-154.

Van der Hof (1997) - S. van der Hof, De juridische status van de digitale handtekening (The legal status of the digital signature), ITeR-serie nr. 7,

Samsom Bedrijfsinformatie bv Alphen aan den Rijn, 1997, pp. 3-68. A summary is on-line available at: <http://cwis.kub.nl/~frw/people/hof/digsig.htm>.

Huydecoper & Van Esch (1997) - Geschriften en handtekeningen: een achterhaald concept? (Writings and signatures: an outdated concept?), ITeR-serie nr. 7, Samsom Bedrijfsinformatie bv Alphen aan den Rijn, 1997, p. 69-162.

IVIR (1998) - Institute for Information Law, The Law and Practice of Digital Encryption, Amsterdam, May 1998.

Kralingen / Prins / Grijpink (1997) - R.W. van Kralingen, J.E.J. Prins, J.H.A.M. Grijpink, Het lichaam als sleutel. Juridische beschouwingen over biometrie. (Using your body as a key. Legal aspects of biometrics), ITeR-serie nr.8, Samsom Bedrijfsinformatie bv, Alphen aan de Rijn, 1997.

Kuner (1998) - C. Kuner, *The Emerging European Legal Framework for Digital Signatures*, BNA's Electronic, Commerce & Law Report, 27 May 1998, p. 712-716.

Kuner & Miedbrodt (1999) - C. Kuner, A. Miedbrodt, *Written Signature Requirements and Electronic Authentication: A Comparative Perspective*, The EDI Law Review 2/3 1999, p.143-154, on-line available at: <http://www.kuner.com/data/sig/signature_perspective.html>.

Matthijssen (1997) - L. Matthijssen, *Legal forms, legal model documents on the Internet*, R&EM, 1997, nr.3, p.19-21.

Roßnagel (1997) - A. Roßnagel, *Das Signaturgesetz. Eine kritische Bewertung des Gesetzentwurfs der Bundesregierung*, DuD 21 (1997) 2, p 75-81.

Schneier (1996) B. Schneier, Applied Cryptography, John Wiley & Sons, Inc, New York 1996.

Schulzki-Haddouti (1999) Ch. Schulzki-Haddouti, *Markt- oder Staatsmacht, Streit um digitale Signaturen*, C T, Magazin für Computer Technik 1/99, p. 58, on-line available at: <http://www.heise.de/ct/99/01/058/>.

Stuyt (1999) - R.A.E. Stuyt, *Technologiespecifieke regelgeving* (Technology-specific legislation), AMI 1999-2, p.17-21.

Tikwart (1998) A. Tikwart J.D, *The Admissibility of Digital Signatures and E-cash in Relation tot the Statute of Fraudes*, MBA 1998, on-line available at: <http://raven.cc.ukans.edu/~cybermom/CLJ/tickwart.html>.

6.2 Other documents

Australia (1997) - Regulatory Efficiency Legislation, Law Reform Committee, Australia, October 1997, on-line available at:
<http://www.parliament.vic.gov.au/lawreform/ref/default.htm>.

Australia (1998) - Electronic Commerce: Building the Legal Framework, Report of the Electronic Commerce Expert Group to the Attorney General, 31 March 1998, on-line available at:
<http://law.gov.au/aghome/advisory/eceg/ecegreport.html>.

Digital Signature Law Survey (1999) - S. van der Hof, Digital Signature Law Survey, Version 3.6, September 1999, on-line available at:
< http://cwis.kub.nl/~frw/people/hof/ds-lawsu.htm>.

FIPR (1999) Foundation for Policy and Research, Signature Directive Consultation, 2 February 1999, on-line available at:
<http://www.cl.cam.ac.uk/users/rja14/signaturedoc.html>.

Huls-report (1998) MDW-rapport Elektronisch verrichten van rechtshandelingen, Commissie Huls, Maart 1998, on-line available at: <http://www.minjust.nl/c_actual/persber/EINDRAP.htm>.

ILPF report (1998) - ILPF Report *Observations on the State of Self-Regulation of the Internet,* Prepared for the ministerial conference of OECD, Ottawa, Canada, 7-9 October 1998, <http://www.ilpf.org/selfreg/whitepaper.htm>.

ILPF Survey (1999) - ILPF, Survey of International Electronic and Digital Signature Initiatives, 12 April 1999, on-line available at:
<http://www.ilpf.org/digsig/survey.htm>.

IVIR (1998) - The Law and Practice of Digital Encryption, IVIR (Institute for Information Law) Amsterdam, May 1998, p.23.

Memorandum Dutch Cabinet (1998) - Nota *Wetgeving voor de elektronische snelweg* (Memorandum *Legislation for the electronic highway*), Tweede Kamer 1997-1998, 25880.

UNCITRAL Draft Uniform Rules (1999) - UNCITRAL Draft Uniform Rules on Electronic Signatures, A/CN.9/WG.IV/WP.82, 29 June 1999, on-line available at: <http://www.uncitral.org/english/sessions/wg_ec/wp-82.pdf>.

UNCITRAL Model Law (1996) - UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, United Nations, New York, 1997. On-line available at: <http://www.uncitral.org/english/texts/electcom/ml-ec.htm>.

7. Samenvatting

Met de opmars van Electronic Commerce onstaat de behoefte aan elektronische alternatieven voor de handmatige handtekening. In deze studie wordt onder de term Electronic Commerce verstaan: zakendoen op het Internet. De sterke toename van het commerciële gebruik van het Internet heeft ervoor gezorgd dat overheden, bedrijven en Internet gebruikers steeds vaker geconfronteerd werden met een scala een juridische rechtsvragen. Eén van de belangrijkste vragen die in dit verband opkomt is de vraag wat de juridische status is van elektronische of digitale handtekeningen.

Dit onderzoek bouwt voort op twee eerder verschenen ITeR onderzoeken: *De juridische status van digitale handtekeningen* door Van der Hof (1997), alsmede *Geschriften en handtekeningen: een achterhaald concept?* door Huydecoper & Van Esch.(1997). Eerst genoemde studie inventariseert de juridische ontwikkelingen en praktische initiatieven met betrekking tot digitale handtekeningen in een aantal Europese Lidstaten. De tweede studie analyseert wat geschriften en handtekeningen zijn en met welke reden zij door de Nederlandse wetgever als vormvoorschrift voor het verrichten van een bepaalde rechtshandeling worden voorgeschreven. Vervolgens wordt nader ingegaan op de vraag of rechtshandelingen ten aanzien waarvan in de wet vormvereisten worden gesteld ook elektronisch wijze verricht kunnen worden, alsmede wat de juridische status is van elektronische berichten en elektronische handtekeningen.

Deze bijdrage beoogt een stapje verder te zetten op de digitale handtekeningen-route. Het doel is om aanbevelingen te doen aan de Nederlandse wetgever ten behoeve van de (aanpassing van) wettelijke vormvoorschriften in de Nederlandse wetgeving. Alvorens te komen tot de formulering van deze aanbevelingen is het noodzakelijk om stil te staan bij de context waarin (elektronische) authenticatie plaatsheeft en bij de al uitgevaardigde wetten en regelgeving, alsmede de daarin gekozen benaderingen.

Hiertoe worden allereerst een vijftal algemene topics in kaart gebracht (hoofdstuk 2) die het onderwerp van studie in een breder perspectief plaatsen:

- De aantrekkelijkheid van digitale handtekeningen
- Techniek-onafhankelijkheid versus technologie-afhankelijkheid
- Nationale benaderingen versus internationale benaderingen van elektronische autheticatie
- Civil Law versus Common Law
- Regulering versus zelfregulering

In hoofdstuk 3 worden vervolgens de benaderingen met betrekking tot wetgeving en regulering van elektronische authenticatie geïdentificeerd alsmede geanalyseerd.

De volgende drie benaderingen worden onderscheiden:

- De digitale handtekening-benadering
- De tweetraps-benadering
- De minimalistische benadering

Het hoofdstuk wordt afgesloten met een synthese en evaluatie van deze benaderingen, alsmede met onze tussenconclusie. In deze tussenconclusie geven wij de voorkeur aan de minimalistische benadering. Deze benadering biedt namelijk rechtszekerheid voor de markt zonder nieuwe technologische ontwikkelingen te belemmeren door nodeloos gedetailleerde regelgeving.

In hoofdstuk 4 wordt deze minimalistische benadering nader onder de loep genomen en verder onderverdeeld in de specifieke functionele benadering en de generieke functionele benadering. Na een behandeling en evaluatie van beide benaderingen kiezen wij voor laatstgenoemde benadering. Ofschoon beide benaderingen waardevol zijn bij de aanpak van vormvoorschriften in het licht van ICT, geeft de generieke functionele benadering vooral op de korte termijn een oplossing en biedt deze benadering tevens betere mogelijkheden voor een internationale aanpak van elektronische authenticatie en vormvoorschriften in digitalibus meer in het algemeen.

Aan de hand van de voorgaande hoofdstukken formuleren wij de resultaten van dit onderzoek als aanbevelingen voor de wetgever. Aan de hand van deze aanbevelingen wordt duidelijk hoe de overheid in onze visie dient om te gaan met de wettelijke vormvereisten in het licht van ICT. De wegever zal allereerst de terminologie rondom het onderwerp elektronische authenticatie moeten beheersen en de wisselende context waarin vormvoorschriften kunnen worden geplaatst goed in het oog dienen te houden. Samenwerking met wetenschap en bedrijfsleven zijn daarbij van groot belang. Bij het daadwerkelijk ontwikkelen

van wetgevingsactiviteiten zal de wetgever ten slotte een minimalistische beandering moeten kiezen om ruimte te laten voor nieuwe ontwikkelingen in een markt die continu in beweging is.

Auteurs

Mr B.P. Aalberts

Babette Aalberts studeerde Nederlands Recht in Leiden. Sinds 1998 is zij als toegevoegd onderzoekster verbonden aan het Centrum voor Recht, Bestuur en Informatisering van de Katholieke Universiteit Brabant. Zij houdt zich bezig met onderzoek op verschillende terreinen die samenhangen met informatie(technologie) en recht. Haar onderzoek concentreert zich momenteel op de volgende onderwerpen: auteurs- en mediarecht, digitale handtekeningen, de databankenwet en domeinnamen. Babette is tevens advocaat bij Kennedy Van der Laan te Amsterdam. On-line informatie is beschikbaar op: <http://law.kub.nl/users/aalberts>

Mr S. van der Hof

Simone van der Hof studeerde Nederlands recht (privaat- en strafrechtelijke rechtspraktijk, met als specialisatie auteursrecht) aan de Universiteit Utrecht. Aansluitend was zij in het kader van het TEDIS-project van de Europese Commissie als onderzoeker verbonden aan het Molengraaff Instituut voor Privaatrecht van de Universiteit Utrecht. Zij is thans onderzoeker bij het Centrum voor Recht, Bestuur en Informatisering van de Katholieke Universiteit Brabant. Haar onderzoeksgebieden zijn: (1) de privaatrechtelijk aspecten van de elektronische handel in het algemeen en meer specifiek de internationale on-line overeenkomst en digitale handtekeningen en (2) overheidsinformatie alsmede pluriformiteit in informatievoorziening. On-line informatie is beschikbaar op: <http://law.kub.nl/users/hof>.